



US 20020007456A1

(19) United States

(12) Patent Application Publication

Peinado et al.

(10) Pub. No.: US 2002/0007456 A1

(43) Pub. Date: Jan. 17, 2002

(54) SECURE PROCESSOR ARCHITECTURE
FOR USE WITH A DIGITAL RIGHTS
MANAGEMENT (DRM) SYSTEM ON A
COMPUTING DEVICE

Publication Classification

(51) Int. Cl.⁷ H04L 9/00
(52) U.S. Cl. 713/164

(76) Inventors: Marcus Peinado, Bellevue, WA (US);
Paul England, Bellevue, WA (US)

(57) ABSTRACT

Correspondence Address:
WOODCOCK WASHBURN KURTZ
MACKIEWICZ & NORRIS LLP
ATTENTION: STEVEN J. ROCCI, ESQ.
ONE LIBERTY PLACE, 46TH FLOOR
PHILADELPHIA, PA 19103 (US)

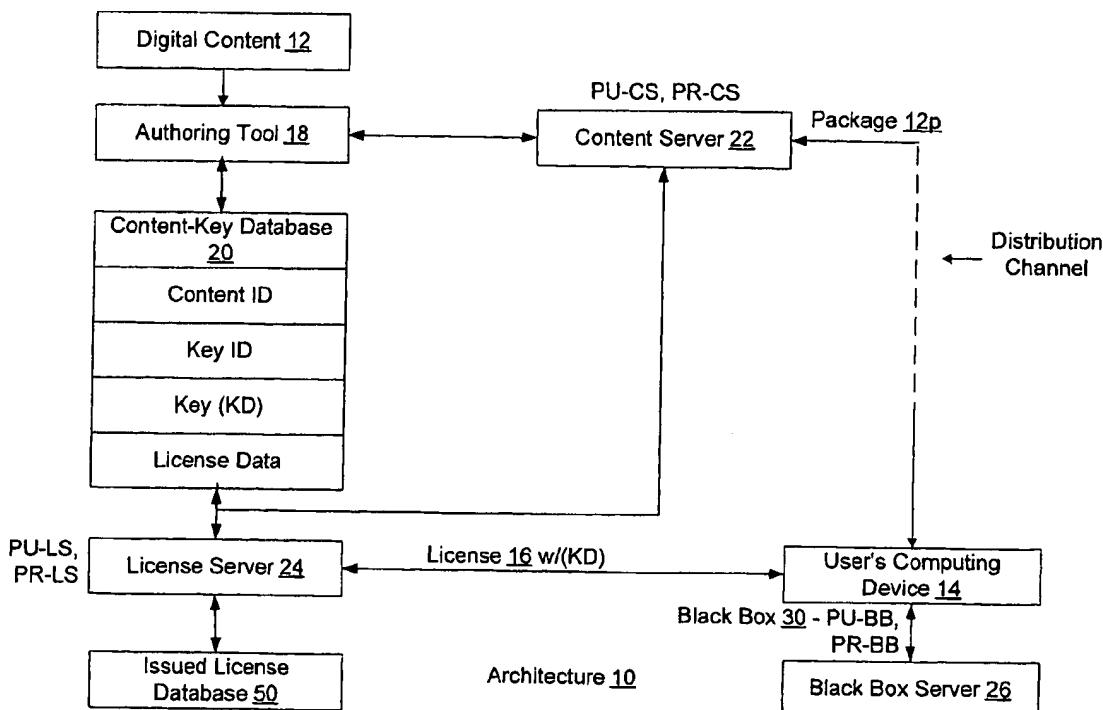
A secure processor is operable in normal and preferred modes, and includes a security kernel instantiated when the processor enters into preferred mode and a security key accessible by the security kernel during preferred mode. The security kernel employs the accessed security key to authenticate a secure application, and allows the processor to be trusted to keep hidden a secret of the application. To instantiate the application, the processor enters preferred mode where the security key is accessible, and instantiates and runs the security kernel. The security kernel accesses the security key and applies same to decrypt a key for the application, stores the decrypted key in a location where the application will expect same, and instantiates the application. The processor then enters the normal mode, where the security key is not accessible.

(21) Appl. No.: 09/892,329

(22) Filed: Jun. 27, 2001

Related U.S. Application Data

(63) Non-provisional of provisional application No. 60/126,614, filed on Mar. 27, 1999.



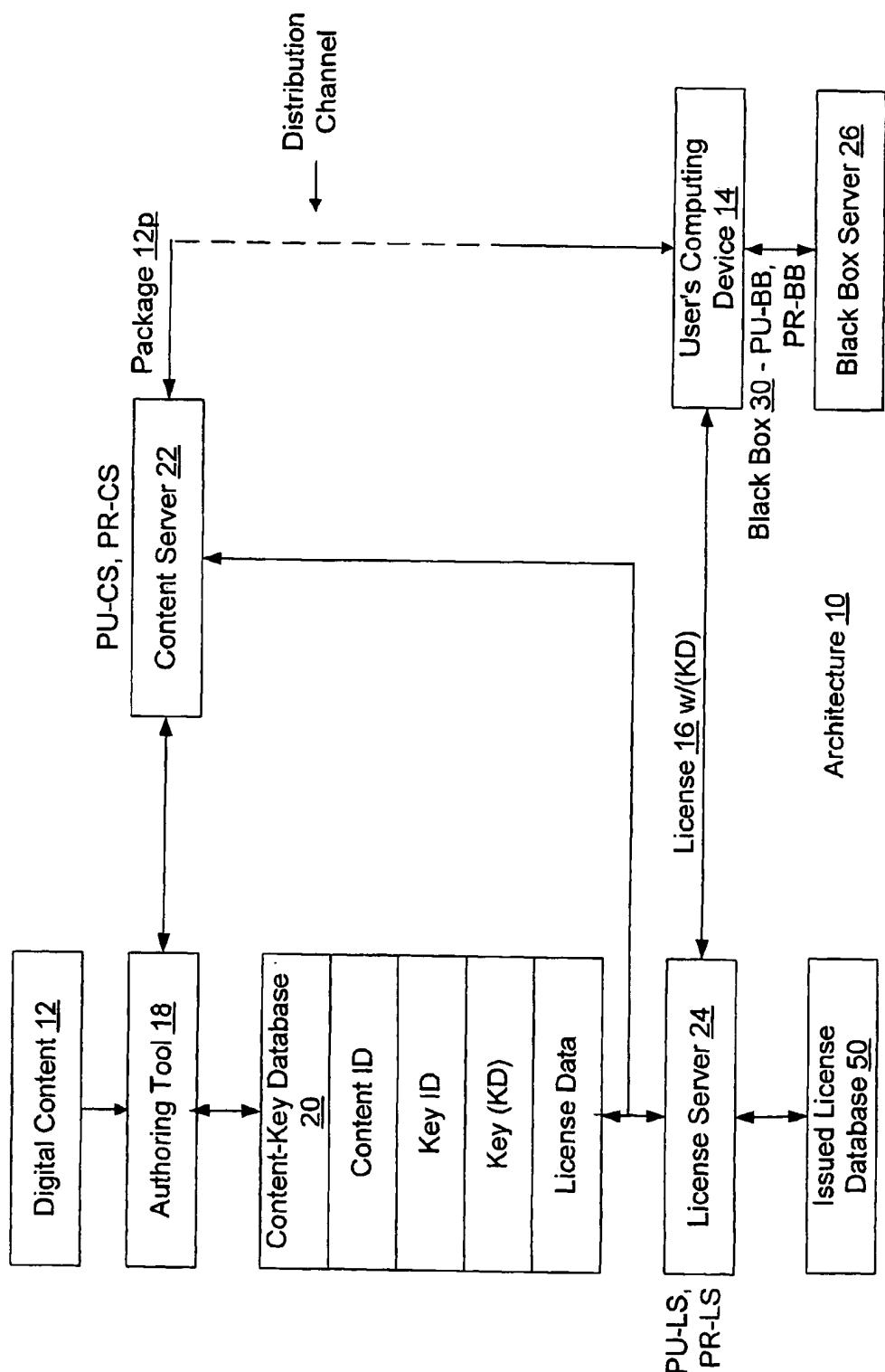
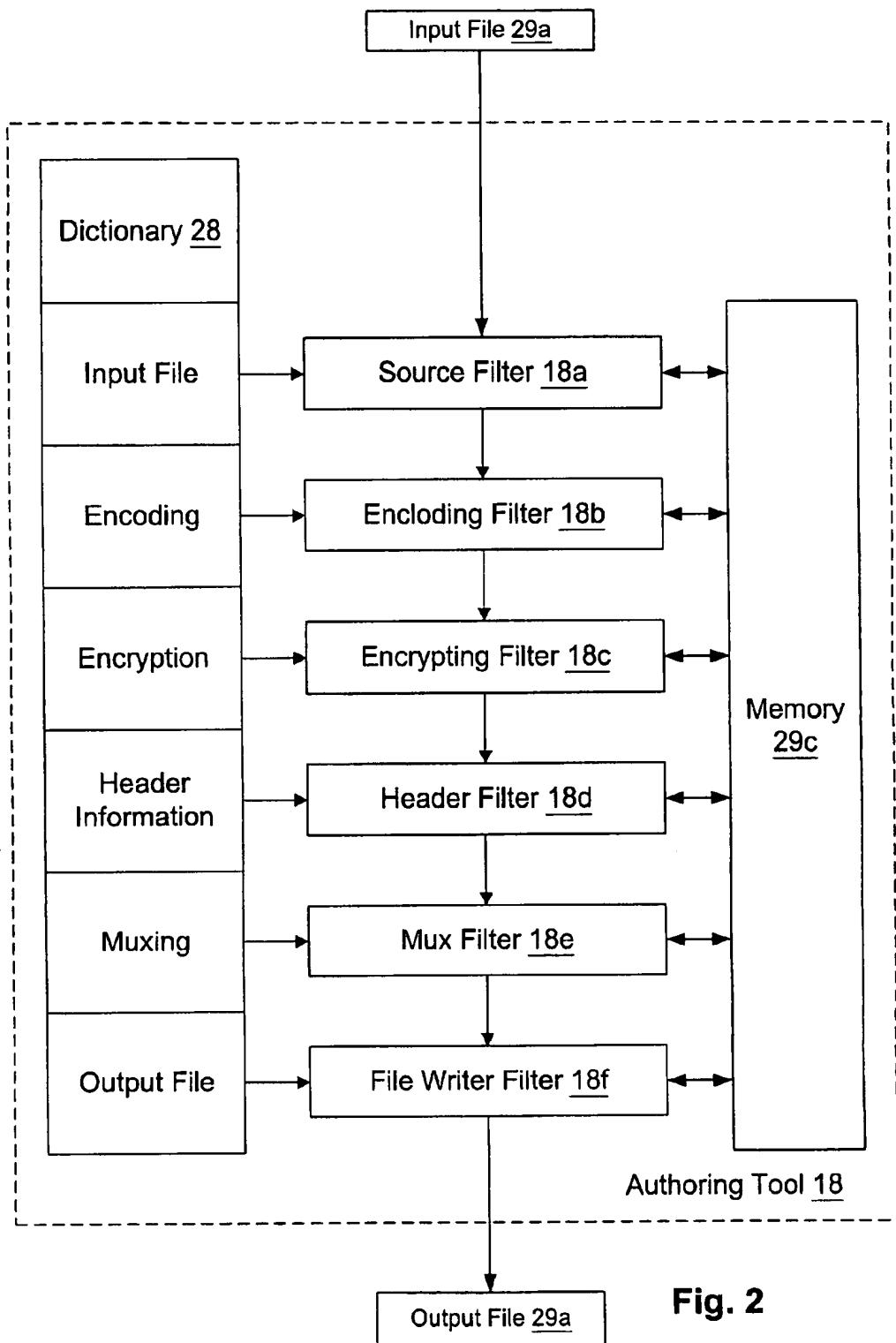


Fig. 1



License <u>16</u>	Content ID	DRL <u>48</u> or KD (DRL <u>48</u>)	PU-BB (KD)	S (PR-LS)	CERT (PU-LS) S (PR-CS)
-------------------	------------	--------------------------------------	------------	-----------	------------------------

Fig. 3

Digital Content Package <u>12p</u>	KD (Digital Content <u>12</u>)	Content ID	Key ID	License Acquisition Info	KD (PU-CS) S (PR-CS)
---------------------------------------	---------------------------------	------------	--------	--------------------------	----------------------

Fig. 8

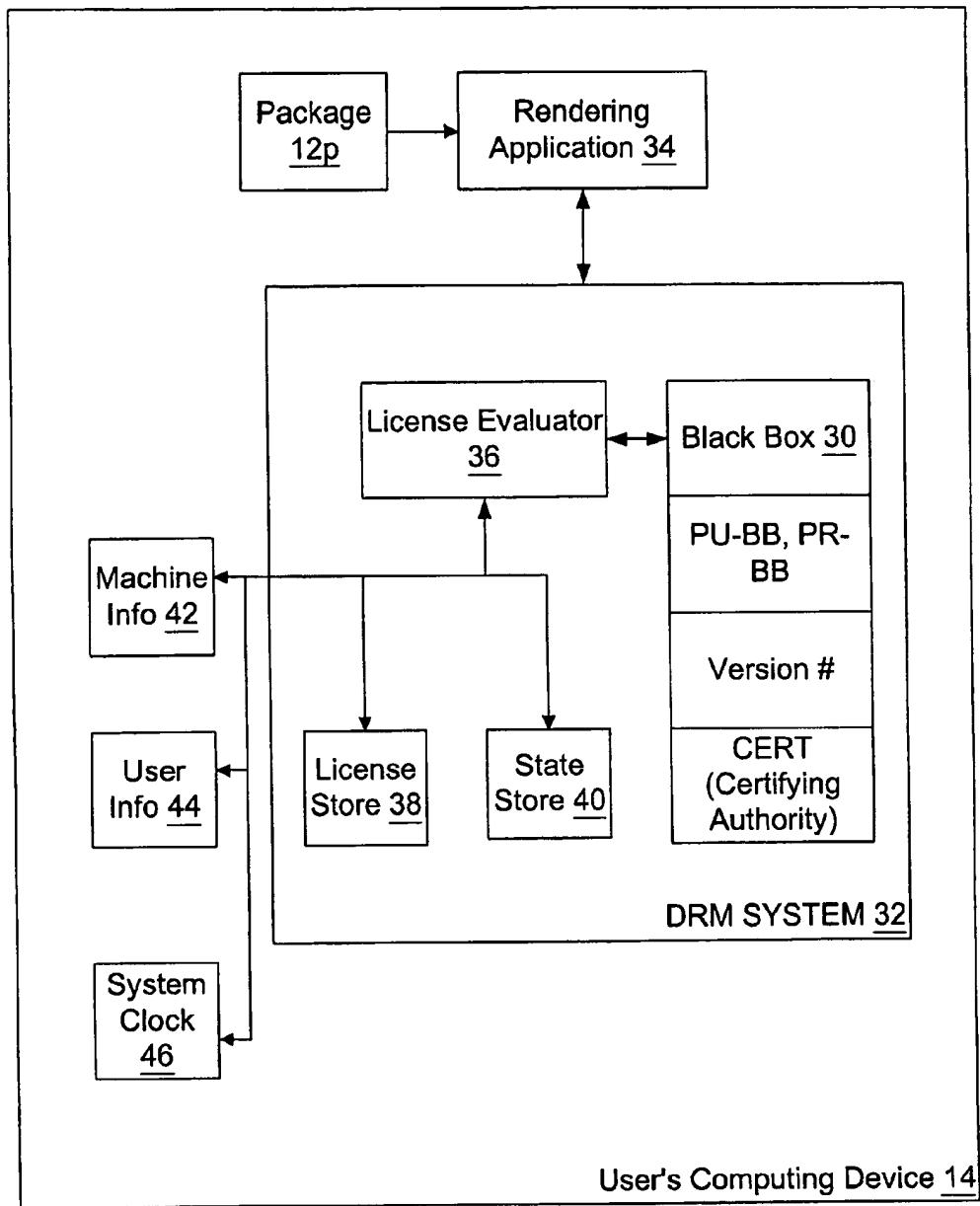
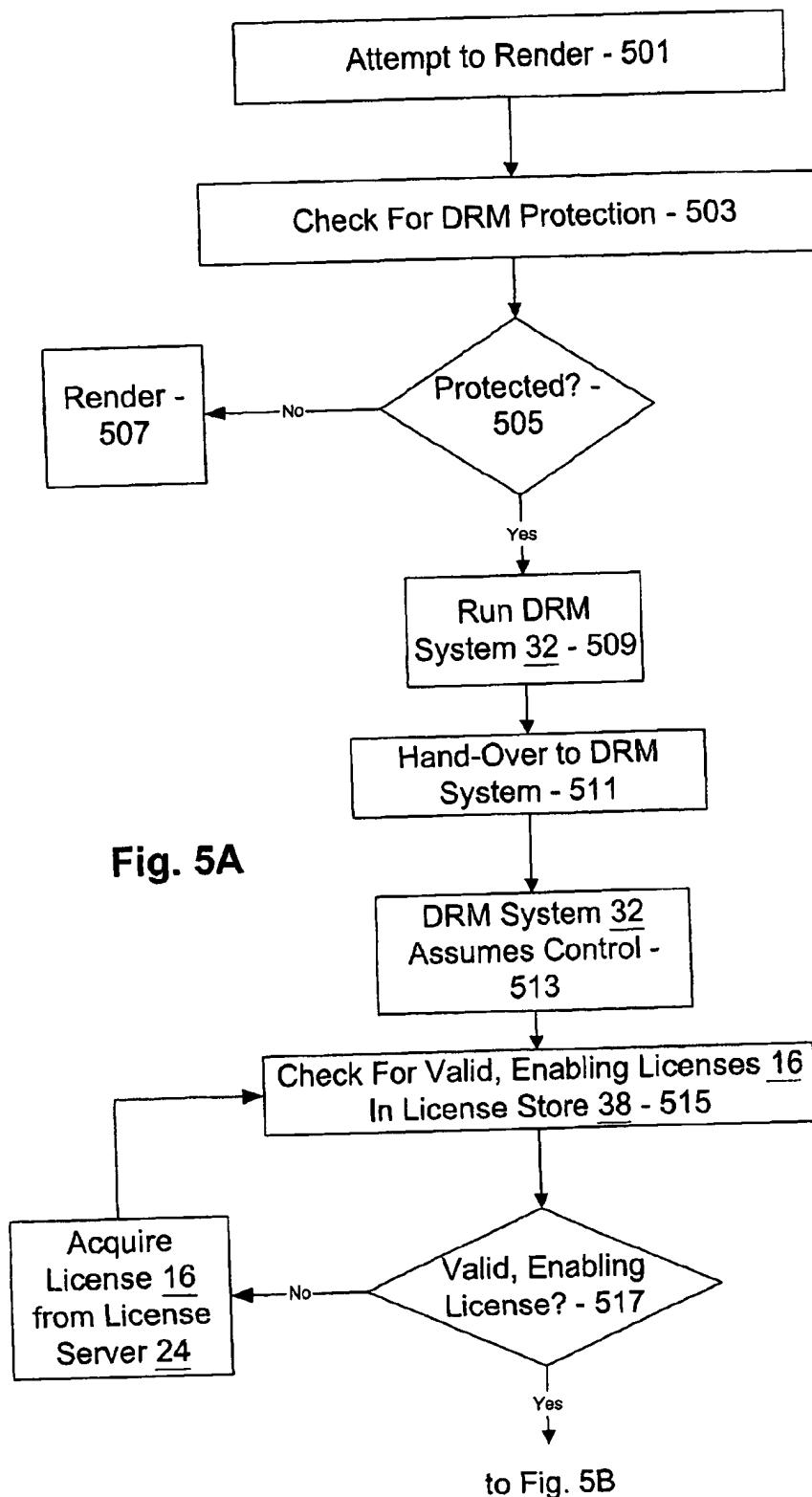


Fig. 4



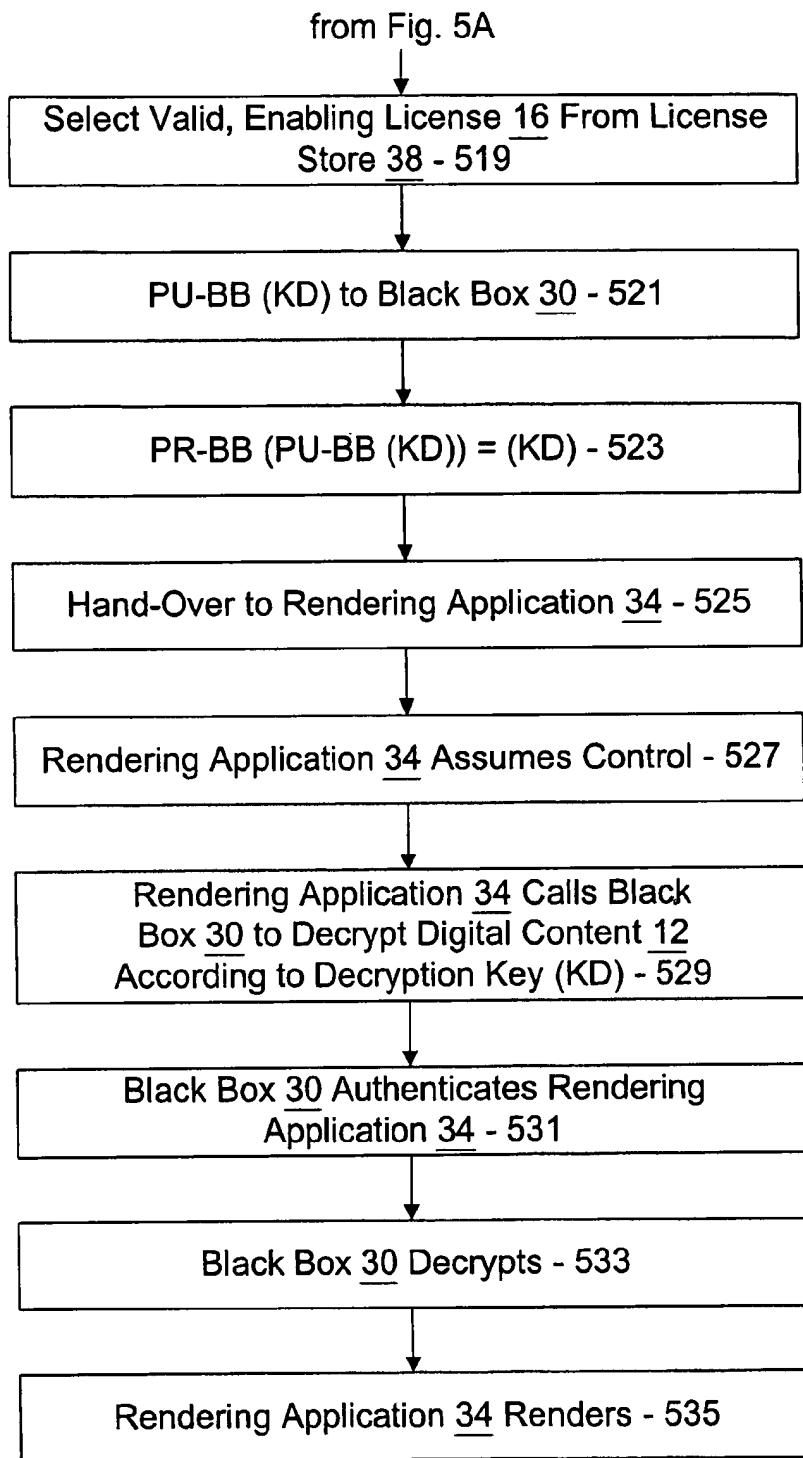


Fig. 5B

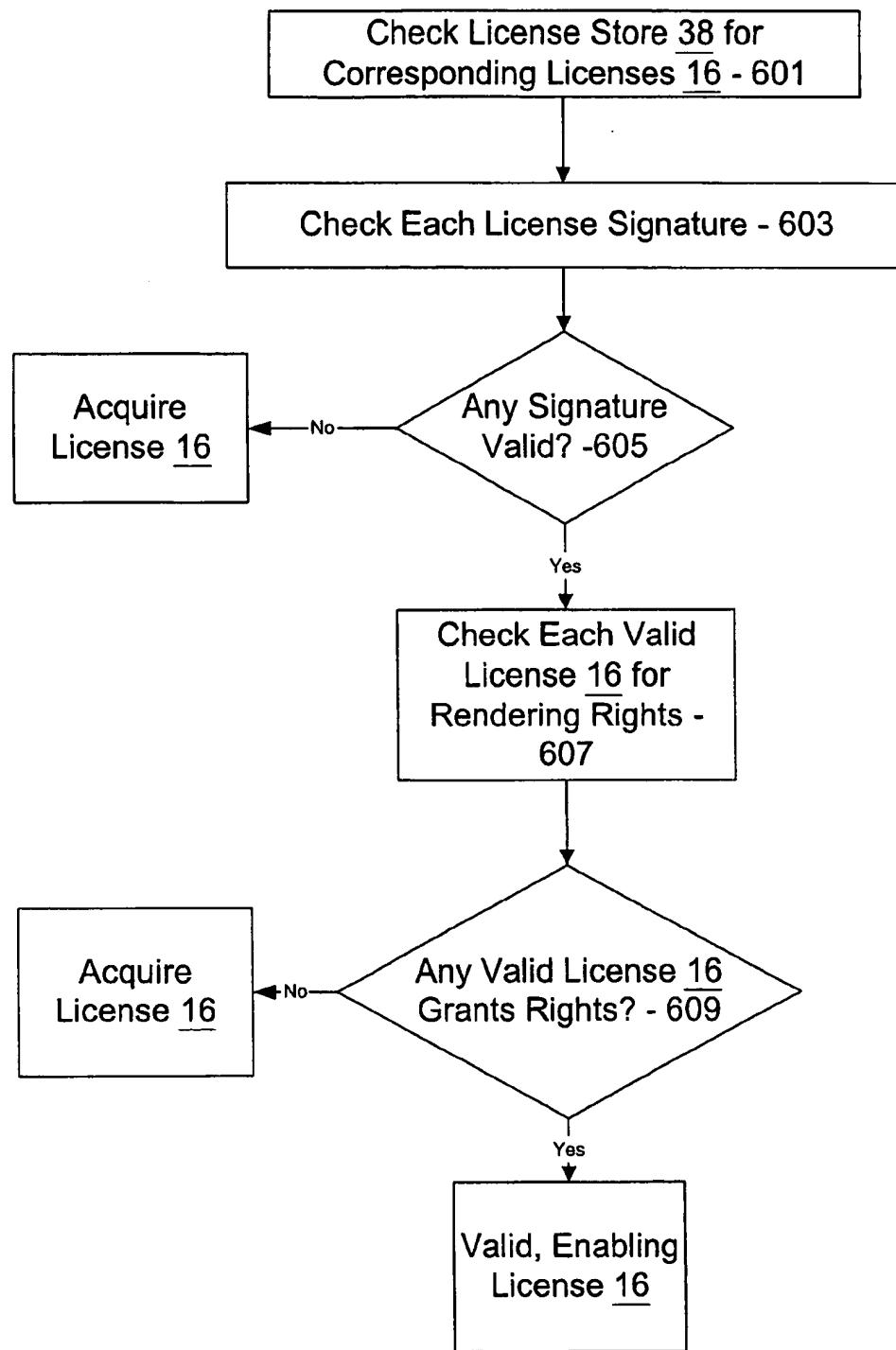


Fig. 6

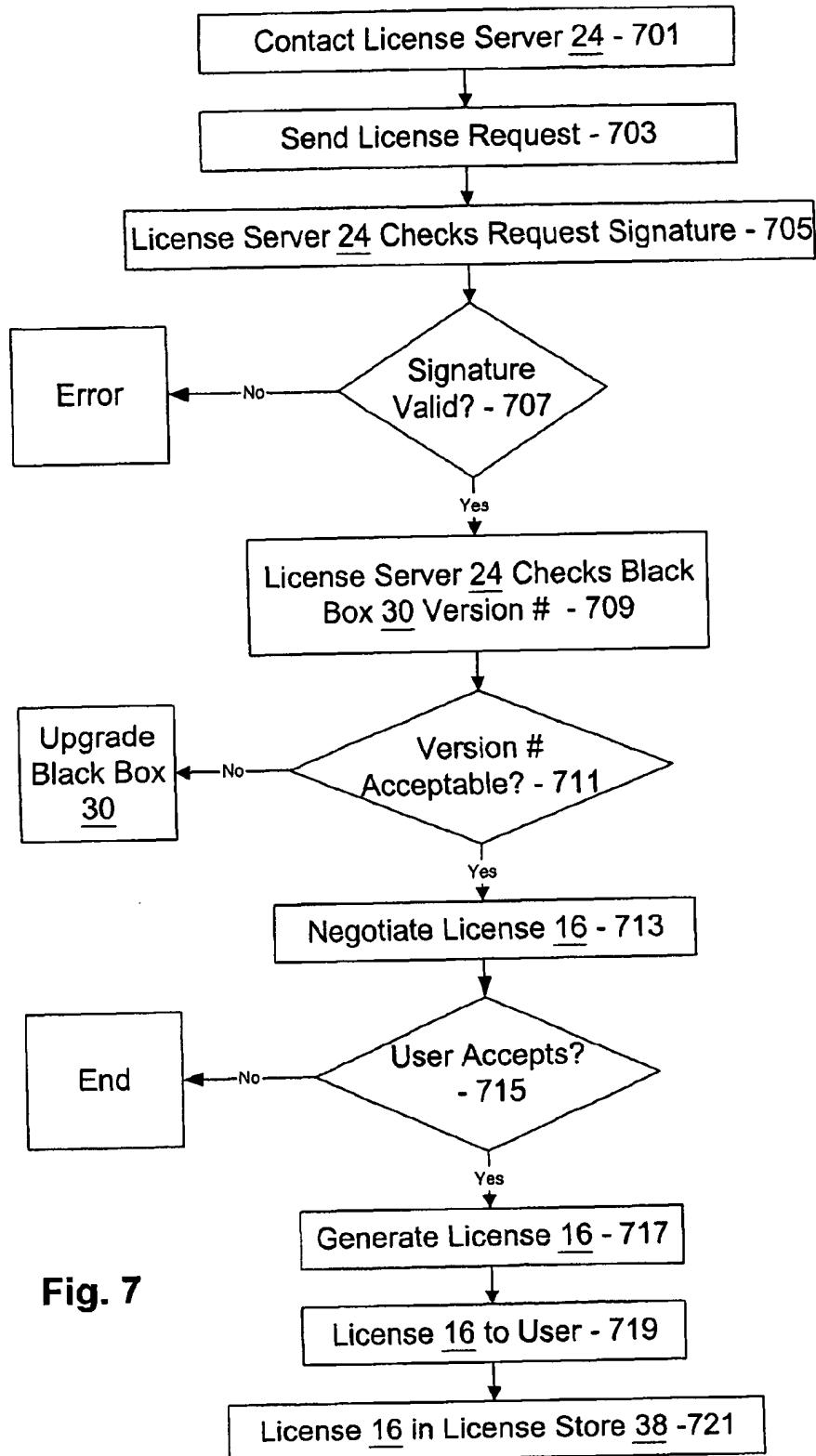


Fig. 7

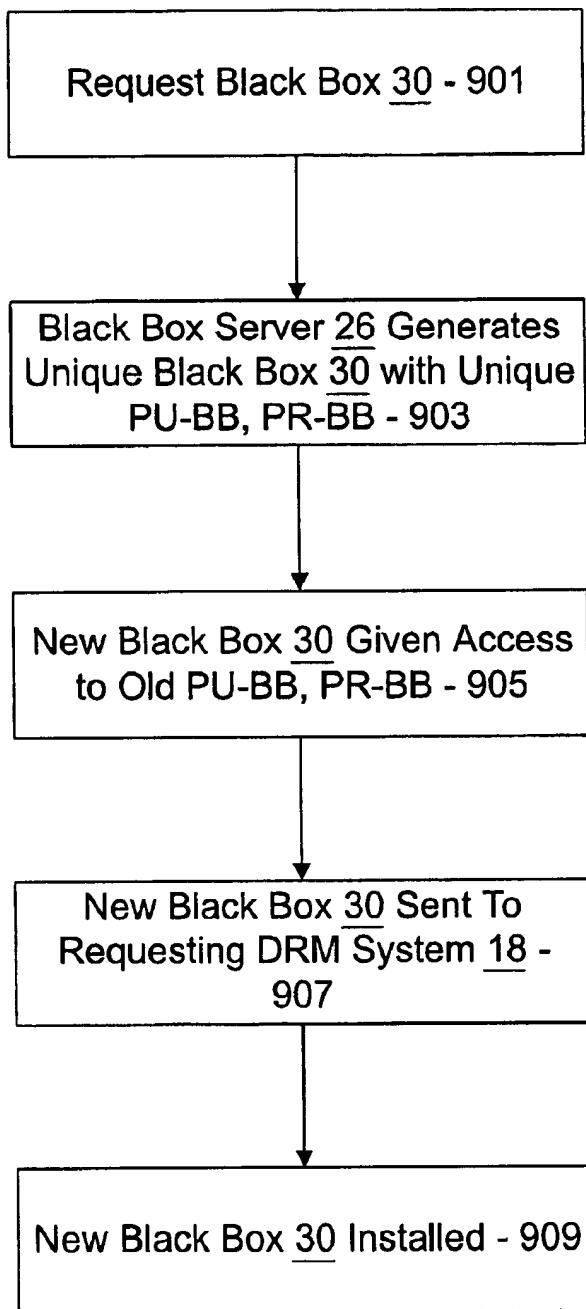


Fig. 9

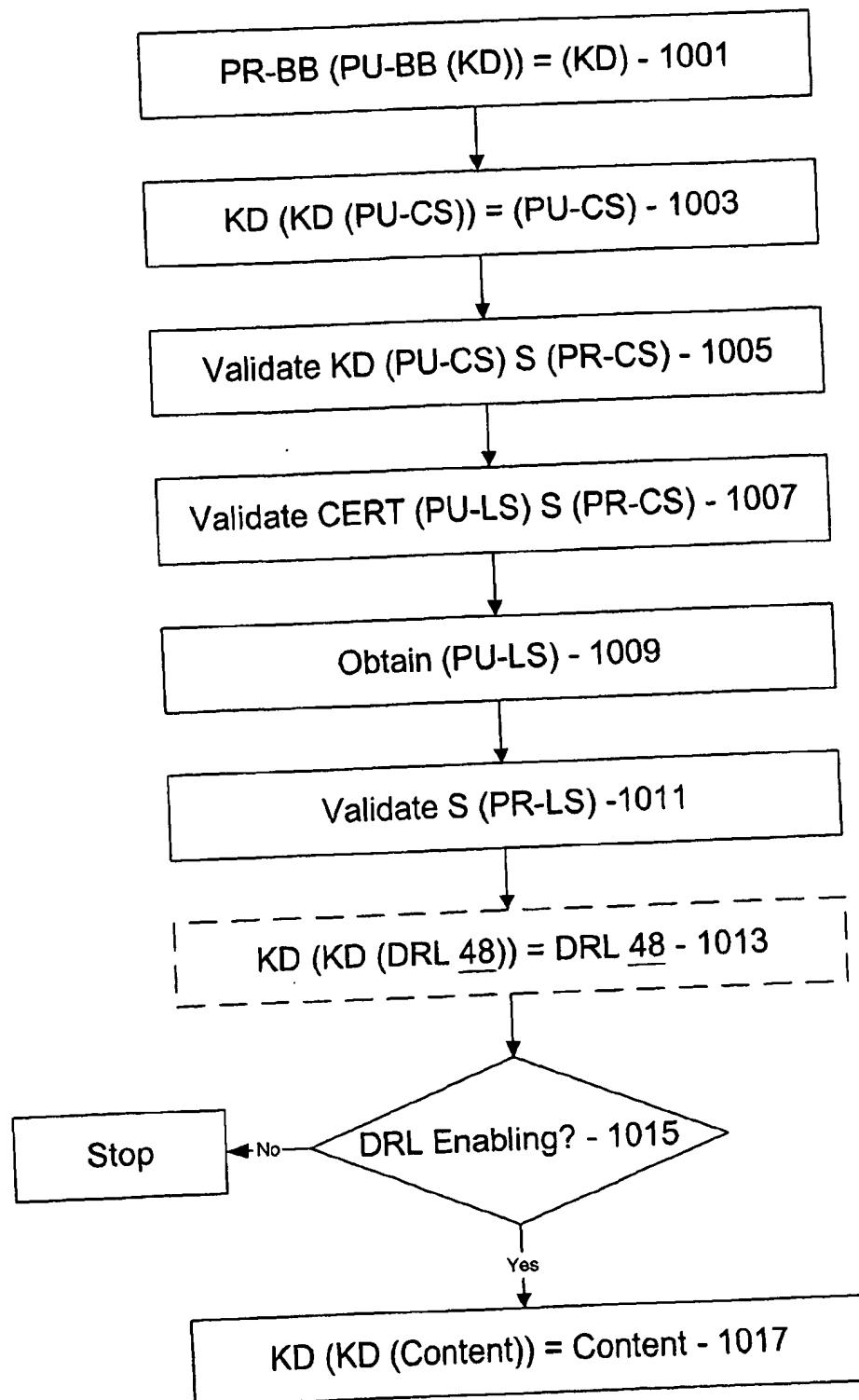


Fig. 10

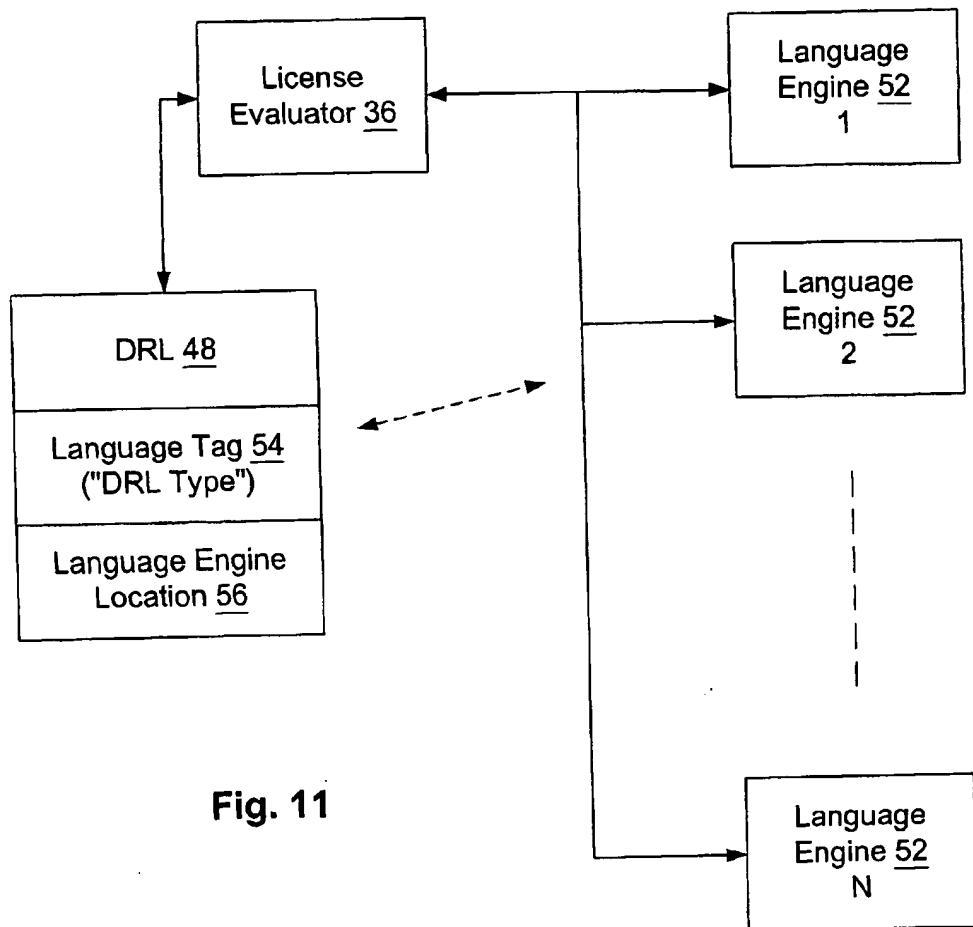


Fig. 11

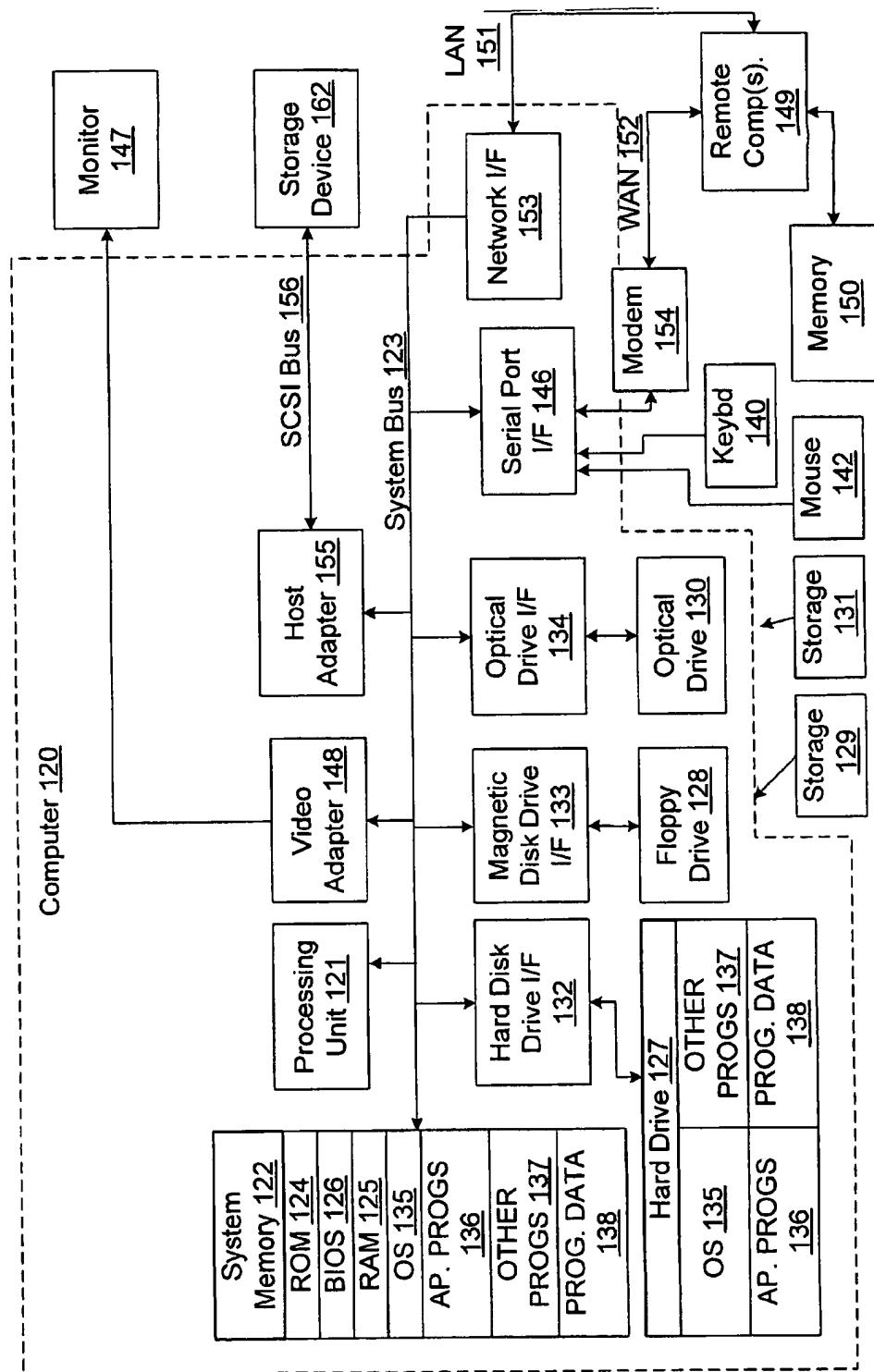


Fig. 12

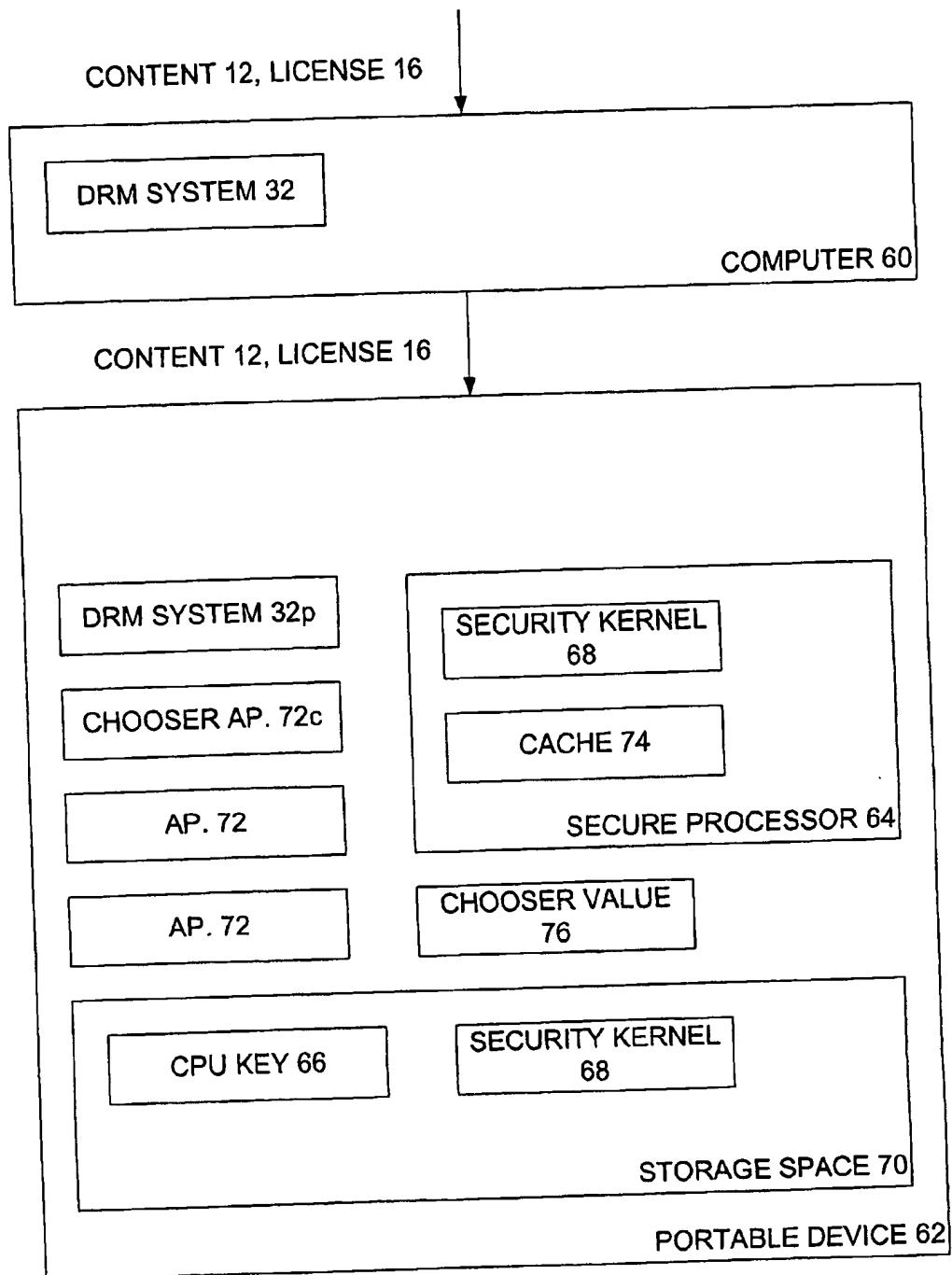


Fig. 13

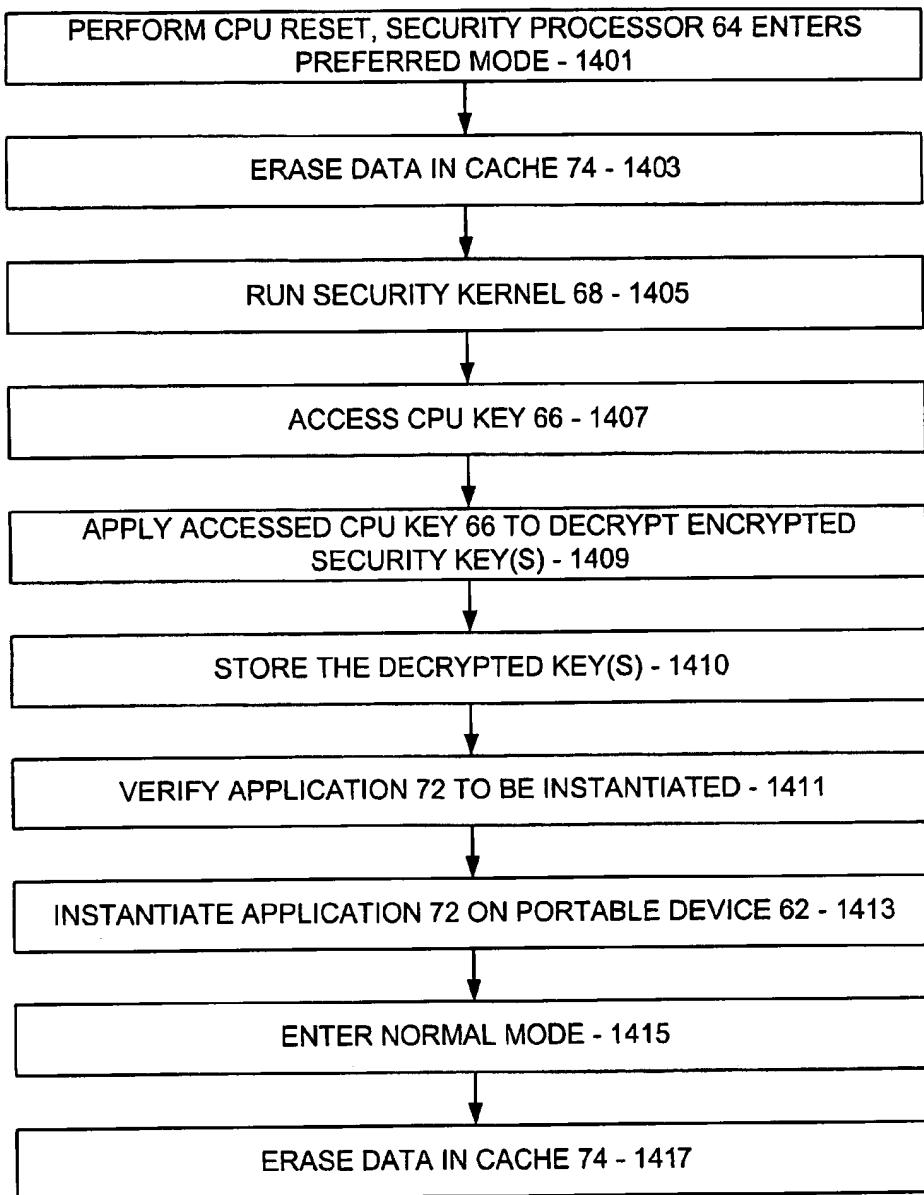


FIG. 14

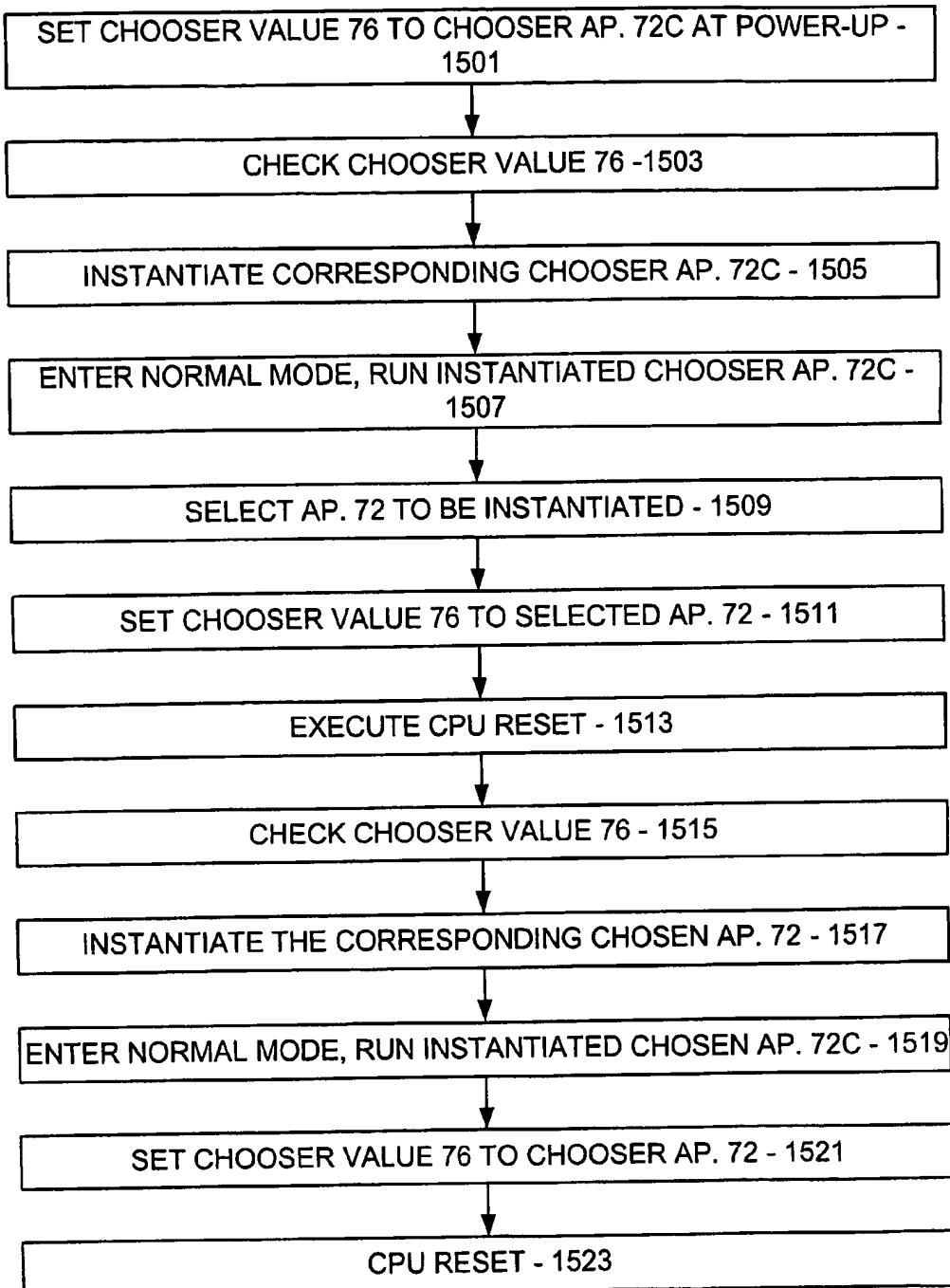


FIG. 15

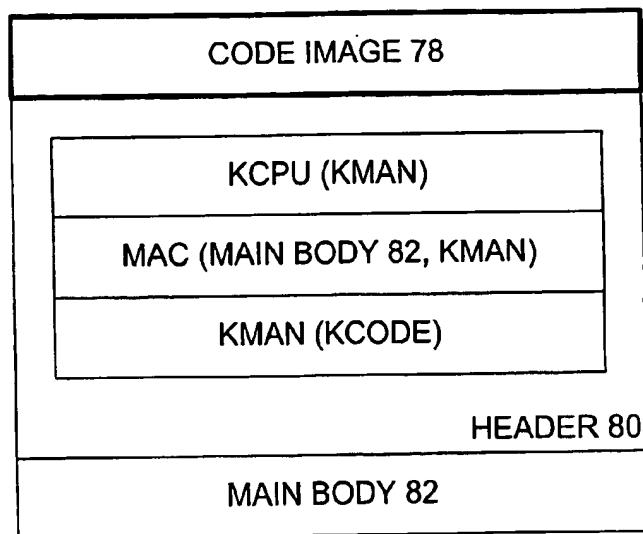


Fig. 16

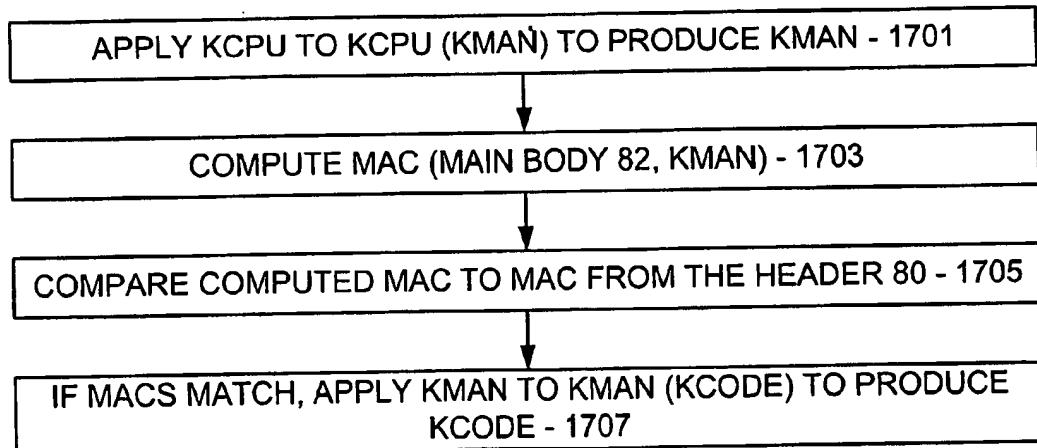


FIG. 17

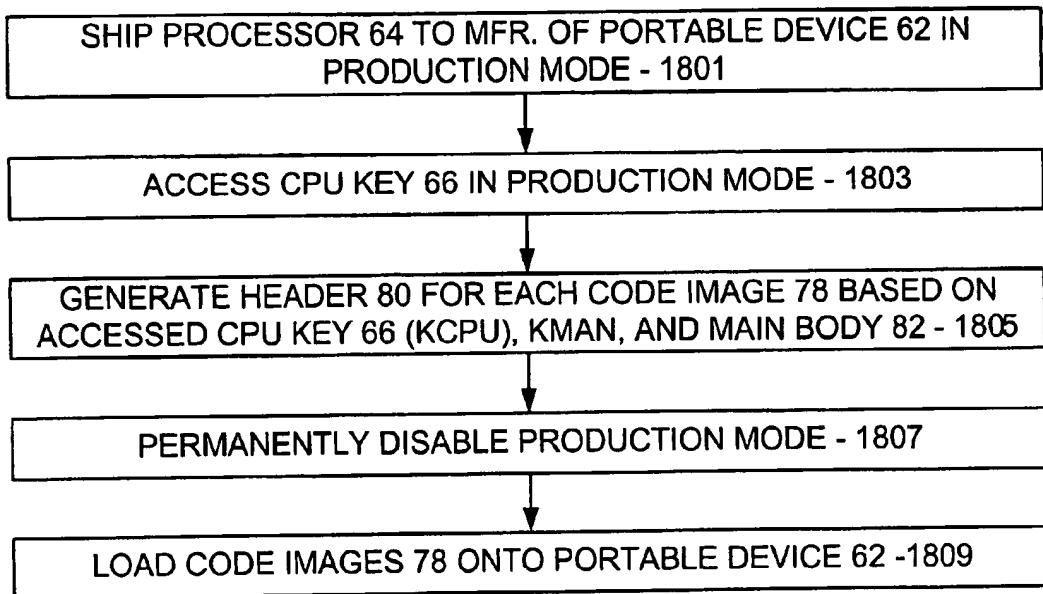


FIG. 18

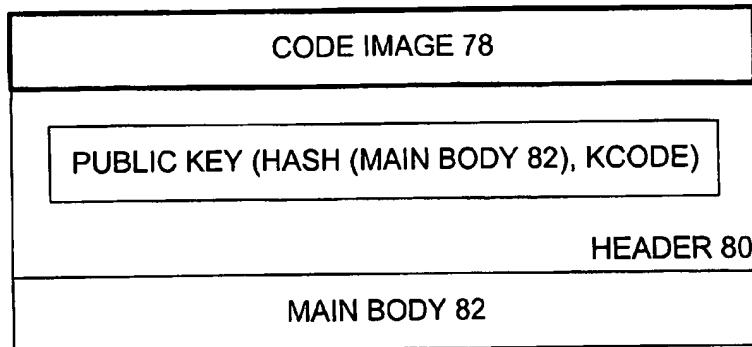


Fig. 19

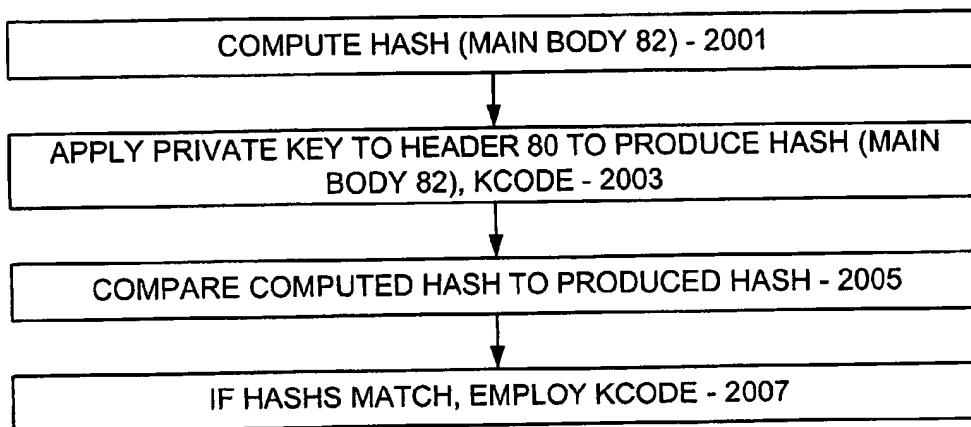


FIG. 20

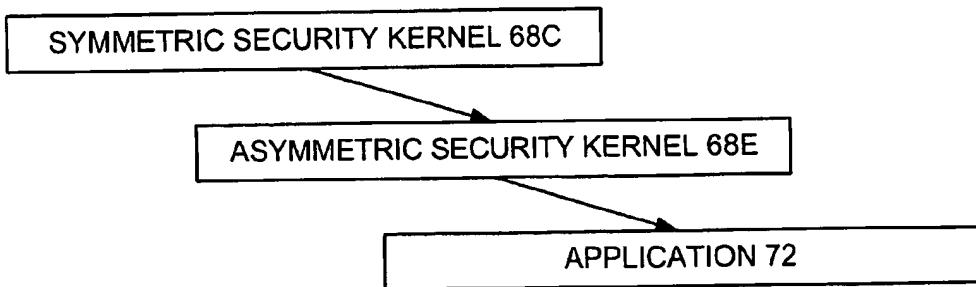


FIG. 21

**SECURE PROCESSOR ARCHITECTURE FOR USE
WITH A DIGITAL RIGHTS MANAGEMENT (DRM)
SYSTEM ON A COMPUTING DEVICE****BACKGROUND OF THE INVENTION**

[0001] Digital rights management and enforcement is highly desirable in connection with digital content such as digital audio, digital video, digital text, digital data, digital multimedia, etc., where such digital content is to be distributed to users. Typical modes of distribution include tangible devices such as a magnetic (floppy) disk, a magnetic tape, an optical (compact) disk (CD), etc., and intangible media such as an electronic bulletin board, an electronic network, the Internet, etc. Upon being received by the user, such user renders or 'plays' the digital content with the aid of an appropriate rendering device such as a media player on a personal computer or the like.

[0002] Typically, a content owner or rights-owner, such as an author, a publisher, a broadcaster, etc. (hereinafter "content owner"), wishes to distribute such digital content to a user or recipient in exchange for a license fee or some other consideration. Such content owner, given the choice, would likely wish to restrict what the user can do with such distributed digital content. For example, the content owner would like to restrict the user from copying and re-distributing such content to a second user, at least in a manner that denies the content owner a license fee from such second user.

[0003] In addition, the content owner may wish to provide the user with the flexibility to purchase different types of use licenses at different license fees, while at the same time holding the user to the terms of whatever type of license is in fact purchased. For example, the content owner may wish to allow distributed digital content to be played only a limited number of times, only for a certain total time, only on a certain type of machine, only on a certain type of media player, only by a certain type of user, etc.

[0004] However, after distribution has occurred, such content owner has very little if any control over the digital content. This is especially problematic in view of the fact that practically every new or recent personal computer includes the software and hardware necessary to make an exact digital copy of such digital content, and to download such exact digital copy to a write-able magnetic or optical disk, or to send such exact digital copy over a network such as the Internet to any destination.

[0005] Of course, as part of the legitimate transaction where the license fee was obtained, the content owner may require the user of the digital content to promise not to re-distribute such digital content. However, such a promise is easily made and easily broken. A content owner may attempt to prevent such re-distribution through any of several known security devices, usually involving encryption and decryption. However, there is likely very little that prevents a mildly determined user from decrypting encrypted digital content, saving such digital content in an un-encrypted form, and then re-distributing same.

[0006] A need exists, then, for providing an enforcement architecture and method that allows the controlled rendering or playing of arbitrary forms of digital content, where such control is flexible and definable by the content owner of such

digital content. A need also exists for providing a controlled rendering environment on a computing device such as a personal computer, where the rendering environment includes at least a portion of such enforcement architecture. Such controlled rendering environment allows that the digital content will only be rendered as specified by the content owner, even though the digital content is to be rendered on a computing device which is not under the control of the content owner.

[0007] Further, a need exists for a trusted component running on the computing device, where the trusted component enforces the rights of the content owner on such computing device in connection with a piece of digital content, even against attempts by the user of such computing device to access such digital content in ways not permitted by the content owner. As but one example, such a trusted software component prevents a user of the computing device from making a copy of such digital content, except as otherwise allowed for by the content owner thereof.

[0008] Finally, a need exists for a secure processor and an architecture therefor that can be trusted to keep hidden a secret of the trusted component, especially in cases where the processor is on a portable device or the like.

SUMMARY OF THE INVENTION

[0009] The aforementioned needs are satisfied at least in part by an enforcement architecture and method for digital rights management, where the architecture and method enforce rights in protected (secure) digital content available on a medium such as the Internet, an optical disk, etc. For purposes of making content available, the architecture includes a content server from which the digital content is accessible over the Internet or the like in an encrypted form. The content server may also supply the encrypted digital content for recording on an optical disk or the like, wherein the encrypted digital content may be distributed on the optical disk itself. At the content server, the digital content is encrypted using an encryption key, and public/private key techniques are employed to bind the digital content with a digital license at the user's computing device or client machine.

[0010] When a user attempts to render the digital content on a computing device, the rendering application invokes a Digital Rights Management (DRM) system on such user's computing device. If the user is attempting to render the digital content for the first time, the DRM system either directs the user to a license server to obtain a license to render such digital content in the manner sought, or transparently obtains such license from such license server without any action necessary on the part of the user. The license includes:

[0011] a decryption key (KD) that decrypts the encrypted digital content;

[0012] a description of the rights (play, copy, etc.) conferred by the license and related conditions (begin date, expiration date, number of plays, etc.), where such description is in a digitally readable form; and

[0013] a digital signature that ensures the integrity of the license.

[0014] The user should not be able to decrypt and render the encrypted digital content without obtaining such a license from the license server. The obtained license is stored in a license store in the user's computing device.

[0015] Importantly, the license server only issues a license to a DRM system that is 'trusted' (i.e., that can authenticate itself). To implement 'trust', the DRM system is equipped with a 'black box' that performs decryption and encryption functions for such DRM system. The black box includes a public/private key pair, a version number and a unique signature, all as provided by an approved certifying authority. The public key is made available to the license server for purposes of encrypting portions of the issued license, thereby binding such license to such black box. The private key is available to the black box only, and not to the user or anyone else, for purposes of decrypting information encrypted with the corresponding public key. The DRM system is initially provided with a black box with a public/private key pair, and the user is prompted to download from a black box server an updated secure black box when the user first requests a license. The black box server provides the updated black box, along with a unique public/private key pair. Such updated black box is written in unique executable code that will run only on the user's computing device, and is re-updated on a regular basis.

[0016] When a user requests a license, the client machine sends the black box public key, version number, and signature to the license server, and such license server issues a license only if the version number is current and the signature is valid. A license request also includes an identification of the digital content for which a license is requested and a key ID that identifies the decryption key associated with the requested digital content. The license server uses the black box public key to encrypt the decryption key, and the decryption key to encrypt the license terms, then downloads the encrypted decryption key and encrypted license terms to the user's computing device along with a license signature.

[0017] Once the downloaded license has been stored in the DRM system license store, the user can render the digital content according to the rights conferred by the license and specified in the license terms. When a request is made to render the digital content, the black box is caused to decrypt the decryption key and license terms, and a DRM system license evaluator evaluates such license terms. The black box decrypts the encrypted digital content only if the license evaluation results in a decision that the requester is allowed to play such content. The decrypted content is provided to the rendering application for rendering.

[0018] In the present invention, a secure processor for a computing device is operable in a normal mode and a preferred mode, and includes a security kernel for being instantiated on the processor when the processor enters into the preferred mode and a security key accessible by the instantiated security kernel when the processor is operating in the preferred mode. The security kernel employs the accessed security key during the preferred mode to authenticate a secure application on the computing device, and allows the processor to be trusted to keep hidden a secret of the application.

[0019] To instantiate the secure application, the processor enters the preferred mode where the security key is accessible, and instantiates and runs the security kernel. The

security kernel accesses the security key and applies same to decrypt at least one encrypted key for the application, stores the decrypted key(s) in a location where the application will expect the key(s) to be found, and instantiates and/or authenticates the application on the processor. The processor then enters the normal mode from the preferred mode, where the security key is not accessible, and passes control to the application.

[0020] To instantiate one of a plurality of available secure applications, a chooser value is set to a value corresponding to a chooser application upon power-up, preferred mode is entered upon a power-up CPU reset, and the instantiated security kernel determines that the chooser value corresponds to the chooser application and therefore instantiates same. After the chooser application is instantiated and left to run, normal mode is entered and the chooser application presents the plurality of available applications for selection by a user.

[0021] A selection of one of the presented applications to be instantiated is received, the chooser value is set to a value corresponding to the selected application, preferred mode is entered upon an executed CPU reset, and the instantiated security kernel determines that the chooser value corresponds to the selected application and therefore instantiating same. After the selected application is instantiated and left to run, normal mode is entered.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] The foregoing summary, as well as the following detailed description of the embodiments of the present invention, will be better understood when read in conjunction with the appended drawings. For the purpose of illustrating the invention, there are shown in the drawings embodiments which are presently preferred. As should be understood, however, the invention is not limited to the precise arrangements and instrumentalities shown. In the drawings:

[0023] FIG. 1 is a block diagram showing an enforcement architecture in accordance with one embodiment of the present invention;

[0024] FIG. 2 is a block diagram of the authoring tool of the architecture of FIG. 1 in accordance with one embodiment of the present invention;

[0025] FIG. 3 is a block diagram of a digital content package having digital content for use in connection with the architecture of FIG. 1 in accordance with one embodiment of the present invention;

[0026] FIG. 4 is a block diagram of the user's computing device of FIG. 1 in accordance with one embodiment of the present invention;

[0027] FIGS. 5A and 5B are flow diagrams showing the steps performed in connection with the Digital Rights Management (DRM) system of the computing device of FIG. 4 to render content in accordance with one embodiment of the present invention;

[0028] FIG. 6 is a flow diagram showing the steps performed in connection with the DRM system of FIG. 4 to determine whether any valid, enabling licenses are present in accordance with one embodiment of the present invention;

[0029] FIG. 7 is a flow diagram showing the steps performed in connection with the DRM system of FIG. 4 to obtain a license in accordance with one embodiment of the present invention;

[0030] FIG. 8 is a block diagram of a digital license for use in connection with the architecture of FIG. 1 in accordance with one embodiment of the present invention;

[0031] FIG. 9 is a flow diagram showing the steps performed in connection with the DRM system of FIG. 4 to obtain a new black box in accordance with one embodiment of the present invention;

[0032] FIG. 10 is a flow diagram showing the key transaction steps performed in connection with the DRM system of FIG. 4 to validate a license and a piece of digital content and render the content in accordance with one embodiment of the present invention;

[0033] FIG. 11 is a block diagram showing the license evaluator of FIG. 4 along with a Digital Rights License (DRL) of a license and a language engine for interpreting the DRL in accordance with one embodiment of the present invention;

[0034] FIG. 12 is a block diagram representing a general purpose computer system in which aspects of the present invention and/or portions thereof may be incorporated;

[0035] FIG. 13 is a block diagram showing a portable device coupled to a computer for downloading digital content and a digital license from the computer, where the portable device has a processor that runs a secure kernel in accordance with one embodiment of the present invention;

[0036] FIG. 14 is a flow diagram showing steps performed by the processor and secure kernel of the portable device of FIG. 13 in loading an application in accordance with one embodiment of the present invention;

[0037] FIG. 15 is a flow diagram showing steps performed by the processor and secure kernel of the portable device of FIG. 13 in choosing an application to be loaded in accordance with one embodiment of the present invention;

[0038] FIG. 16 is a block diagram showing a code image of an application to be loaded by the security kernel of FIG. 13 in accordance with one embodiment of the present invention where the security kernel employs symmetric cryptography;

[0039] FIG. 17 is a flow diagram showing steps performed by the security kernel of FIG. 16 in accordance with one embodiment of the present invention;

[0040] FIG. 18 is a flow diagram showing steps performed by a manufacturer of the portable device in one embodiment of the present invention where the security kernel employs symmetric cryptography;

[0041] FIG. 19 is a block diagram showing a code image of an application to be loaded by the security kernel of FIG. 13 in accordance with one embodiment of the present invention where the security kernel employs asymmetric cryptography;

[0042] FIG. 20 is a flow diagram showing steps performed by the security kernel of FIG. 19 in accordance with one embodiment of the present invention; and

[0043] FIG. 21 is a block diagram showing a code security kernel employing symmetric cryptography instantiating an extended security kernel employing asymmetric cryptography, which in turn instantiates an application in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0044] Referring to the drawings in details, wherein like numerals are used to indicate like elements throughout, there is shown in FIG. 1 an enforcement architecture 10 in accordance with one embodiment of the present invention. Overall, the enforcement architecture 10 allows an owner of digital content 12 to specify license rules that must be satisfied before such digital content 12 is allowed to be rendered on a user's computing device 14. Such license rules are embodied within a digital license 16 that the user's computing device 14 (hereinafter, such terms are interchangeable unless circumstances require otherwise) must obtain from the content owner or an agent thereof. The digital content 12 is distributed in an encrypted form, and may be distributed freely and widely. Preferably, the decrypting key (KD) for decrypting the digital content 12 is included with the license 16.

[0045] Computer Environment

[0046] FIG. 12 and the following discussion are intended to provide a brief general description of a suitable computing environment in which the present invention and/or portions thereof may be implemented. Although not required, the invention is described in the general context of computer-executable instructions, such as program modules, being executed by a computer, such as a client workstation or a server. Generally, program modules include routines, programs, objects, components, data structures and the like that perform particular tasks or implement particular abstract data types. Moreover, it should be appreciated that the invention and/or portions thereof may be practiced with other computer system configurations, including hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, mini-computers, mainframe computers and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

[0047] As shown in FIG. 12, an exemplary general purpose computing system includes a conventional personal computer 120 or the like, including a processing unit 121, a system memory 122, and a system bus 123 that couples various system components including the system memory to the processing unit 121. The system bus 123 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The system memory includes read-only memory (ROM) 124 and random access memory (RAM) 125. A basic input/output system 126 (BIOS), containing the basic routines that help to transfer information between elements within the personal computer 120, such as during start-up, is stored in ROM 124.

[0048] The personal computer 120 may further include a hard disk drive 127 for reading from and writing to a hard

disk (not shown), a magnetic disk drive 128 for reading from or writing to a removable magnetic disk 129, and an optical disk drive 130 for reading from or writing to a removable optical disk 131 such as a CD-ROM or other optical media. The hard disk drive 127, magnetic disk drive 128, and optical disk drive 130 are connected to the system bus 123 by a hard disk drive interface 132, a magnetic disk drive interface 133, and an optical drive interface 134, respectively. The drives and their associated computer-readable media provide non-volatile storage of computer readable instructions, data structures, program modules and other data for the personal computer 20.

[0049] Although the exemplary environment described herein employs a hard disk, a removable magnetic disk 129, and a removable optical disk 131, it should be appreciated that other types of computer readable media which can store data that is accessible by a computer may also be used in the exemplary operating environment. Such other types of media include a magnetic cassette, a flash memory card, a digital video disk, a Bernoulli cartridge, a random access memory (RAM), a read-only memory (ROM), and the like.

[0050] A number of program modules may be stored on the hard disk, magnetic disk 129, optical disk 131, ROM 124 or RAM 125, including an operating system 135, one or more application programs 136, other program modules 137 and program data 138. A user may enter commands and information into the personal computer 120 through input devices such as a keyboard 140 and pointing device 142. Other input devices (not shown) may include a microphone, joystick, game pad, satellite disk, scanner, or the like. These and other input devices are often connected to the processing unit 121 through a serial port interface 146 that is coupled to the system bus, but may be connected by other interfaces, such as a parallel port, game port, or universal serial bus (USB). A monitor 147 or other type of display device is also connected to the system bus 123 via an interface, such as a video adapter 148. In addition to the monitor 147, a personal computer typically includes other peripheral output devices (not shown), such as speakers and printers. The exemplary system of FIG. 12 also includes a host adapter 155, a Small Computer System Interface (SCSI) bus 156, and an external storage device 162 connected to the SCSI bus 156.

[0051] The personal computer 120 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 149. The remote computer 149 may be another personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to the personal computer 120, although only a memory storage device 150 has been illustrated in FIG. 12. The logical connections depicted in FIG. 12 include a local area network (LAN) 151 and a wide area network (WAN) 152. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and the Internet.

[0052] When used in a LAN networking environment, the personal computer 120 is connected to the LAN 151 through a network interface or adapter 153. When used in a WAN networking environment, the personal computer 120 typically includes a modem 154 or other means for establishing communications over the wide area network 152, such as the Internet. The modem 154, which may be internal or external,

is connected to the system bus 123 via the serial port interface 146. In a networked environment, program modules depicted relative to the personal computer 120, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

[0053] Architecture

[0054] Referring again to FIG. 1, in one embodiment of the present invention, the architecture 10 includes an authoring tool 18, a content-key database 20, a content server 22, a license server 24, and a black box server 26, as well as the aforementioned user's computing device 14.

[0055] Architecture—Authoring Tool 18

[0056] The authoring tool 18 is employed by a content owner to package a piece of digital content 12 into a form that is amenable for use in connection with the architecture 10 of the present invention. In particular, the content owner provides the authoring tool 18 with the digital content 12, instructions and/or rules that are to accompany the digital content 12, and instructions and/or rules as to how the digital content 12 is to be packaged. The authoring tool 18 then produces a digital content package 12p having the digital content 12 encrypted according to an encryption/decryption key, and the instructions and/or rules that accompany the digital content 12.

[0057] In one embodiment of the present invention, the authoring tool 18 is instructed to serially produce several different digital content 12 packages 12p, each having the same digital content 12 encrypted according to a different encryption/decryption key. As should be understood, having several different packages 12p with the same digital content 12 may be useful for tracking the distribution of such packages 12p/content 12 (hereinafter simply "digital content 12", unless circumstances require otherwise). Such distribution tracking is not ordinarily necessary, but may be used by an investigative authority in cases where the digital content 12 has been illegally sold or broadcast.

[0058] In one embodiment of the present invention, the encryption/decryption key that encrypts the digital content 12 is a symmetric key, in that the encryption key is also the decryption key (KD). As will be discussed below in more detail, such decryption key (KD) is delivered to a user's computing device 14 in a hidden form as part of a license 16 for such digital content 12. Preferably, each piece of digital content 12 is provided with a content ID (or each package 12p is provided with a package ID), each decryption key (KD) has a key ID, and the authoring tool 18 causes the decryption key (KD), key ID, and content ID (or package ID) for each piece of digital content 12 (or each package 12p) to be stored in the content-key database 20. In addition, license data regarding the types of licenses 16 to be issued for the digital content 12 and the terms and conditions for each type of license 16 may be stored in the content-key database 20, or else in another database (not shown). Preferably, the license data can be modified by the content owner at a later time as circumstances and market conditions may require.

[0059] In use, the authoring tool 18 is supplied with information including, among other things:

- [0060] the digital content 12 to be packaged;
- [0061] the type and parameters of watermarking and/or fingerprinting to be employed, if any;
- [0062] the type and parameters of data compression to be employed, if any;
- [0063] the type and parameters of encryption to be employed;
- [0064] the type and parameters of serialization to be employed, if any; and
- [0065] the instructions and/or rules that are to accompany the digital content 12.

[0066] As is known, a watermark is a hidden, computer-readable signal that is added to the digital content 12 as an identifier. A fingerprint is a watermark that is different for each instance. As should be understood, an instance is a version of the digital content 12 that is unique. Multiple copies of any instance may be made, and any copy is of a particular instance. When a specific instance of digital content 12 is illegally sold or broadcast, an investigative authority can perhaps identify suspects according to the watermark/fingerprint added to such digital content 12.

[0067] Data compression may be performed according to any appropriate compression algorithm without departing from the spirit and scope of the present invention. For example, the .mp3 or .wav compression algorithm may be employed. Of course, the digital content 12 may already be in a compressed state, in which case no additional compression is necessary.

[0068] The instructions and/or rules that are to accompany the digital content 12 may include practically any appropriate instructions, rules, or other information without departing from the spirit and scope of the present invention. As will be discussed below, such accompanying instructions/rules/information are primarily employed by the user and the user's computing device 14 to obtain a license 16 to render the digital content 12. Accordingly, such accompanying instructions/rules/information may include an appropriately formatted license acquisition script or the like, as will be described in more detail below. In addition, or in the alternative, such accompanying instructions/rules/information may include 'preview' information designed to provide a user with a preview of the digital content 12.

[0069] With the supplied information, the authoring tool 18 then produces one or more packages 12p corresponding to the digital content 12. Each package 12p may then be stored on the content server 22 for distribution to the world.

[0070] In one embodiment of the present invention, and referring now to FIG. 2, the authoring tool 18 is a dynamic authoring tool 18 that receives input parameters which can be specified and operated on. Accordingly, such authoring tool 18 can rapidly produce multiple variations of package 12p for multiple pieces of digital content 12. Preferably, the input parameters are embodied in the form of a dictionary 28, as shown, where the dictionary 28 includes such parameters as:

- [0071] the name of the input file 29a having the digital content 12;
- [0072] the type of encoding that is to take place

[0073] the encryption/decryption key (KD) to be employed,

[0074] the accompanying instructions/rules/information ('header information') to be packaged with the digital content 12 in the package 12p.

[0075] the type of muxing that is to occur; and

[0076] the name of the output file 29b to which the package 12p based on the digital content 12 is to be written.

[0077] As should be understood, such dictionary 28 is easily and quickly modifiable by an operator of the authoring tool 18 (human or machine), and therefore the type of authoring performed by the authoring tool 18 is likewise easily and quickly modifiable in a dynamic manner. In one embodiment of the present invention, the authoring tool 18 includes an operator interface (not shown) displayable on a computer screen to a human operator. Accordingly, such operator may modify the dictionary 28 by way of the interface, and further may be appropriately aided and/or restricted in modifying the dictionary 28 by way of the interface.

[0078] In the authoring tool 18, and as seen in FIG. 2, a source filter 18a receives the name of the input file 29a having the digital content 12 from the dictionary 28, and retrieves such digital content 12 from such input file and places the digital content 12 into a memory 29c such as a RAM or the like. An encoding filter 18b then performs encoding on the digital content 12 in the memory 29c to transfer the file from the input format to the output format according to the type of encoding specified in the dictionary 28 (i.e., .wav to asp, .mp3 to asp, etc.), and places the encoded digital content 12 in the memory 29c. As shown, the digital content 12 to be packaged (music, e.g.) is received in a compressed format such as the .wav or .mp3 format, and is transformed into a format such as the asp (active streaming protocol) format. Of course, other input and output formats may be employed without departing from the spirit and scope of the present invention.

[0079] Thereafter, an encryption filter 18c encrypts the encoded digital content 12 in the memory 29c according to the encryption/decryption key (KD) specified in the dictionary 28, and places the encrypted digital content 12 in the memory 29c. A header filter 18d then adds the header information specified in the dictionary 28 to the encrypted digital content 12 in the memory 29c.

[0080] As should be understood, depending on the situation, the package 12p may include multiple streams of temporally aligned digital content 12 (one stream being shown in FIG. 2), where such multiple streams are multiplexed (i.e., 'muxed'). Accordingly, a mux filter 18e performs muxing on the header information and encrypted digital content 12 in the memory 29c according to the type of muxing specified in the dictionary 28, and places the result in the memory 29c. A file writer filter 18f then retrieves the result from the memory 29c and writes such result to the output file 29b specified in the dictionary 28 as the package 12p.

[0081] It should be noted that in certain circumstances, the type of encoding to be performed will not normally change. Since the type of muxing typically is based on the type of

encoding, it is likewise the case that the type of muxing will not normally change, either. If this is in fact the case, the dictionary 28 need not include parameters on the type of encoding and/or the type of muxing. Instead, it is only necessary that the type of encoding be 'hardwired' into the encoding filter and/or that the type of muxing be 'hardwired' into the mux filter. Of course, as circumstance require, the authoring tool 18 may not include all of the aforementioned filters, or may include other filters, and any included filter may be hardwired or may perform its function according to parameters specified in the dictionary 28, all without departing from the spirit and scope of the present invention.

[0082] Preferably, the authoring tool 18 is implemented on an appropriate computer, processor, or other computing machine by way of appropriate software. The structure and operation of such machine and such software should be apparent based on the disclosure herein and therefore do not require any detailed discussion in the present disclosure.

[0083] Architecture—Content Server 22

[0084] Referring again to FIG. 1, in one embodiment of the present invention, the content server 22 distributes or otherwise makes available for retrieval the packages 12p produced by the authoring tool 18. Such packages 12p may be distributed as requested by the content server 22 by way of any appropriate distribution channel without departing from the spirit and scope of the present invention. For example, such distribution channel may be the Internet or another network, an electronic bulletin board, electronic mail, or the like. In addition, the content server 22 may be employed to copy the packages 12p onto magnetic or optical disks or other storage devices, and such storage devices may then be distributed.

[0085] It will be appreciated that the content server 22 distributes packages 12p without regard to any trust or security issues. As discussed below, such issues are dealt with in connection with the license server 24 and the relationship between such license server 24 and the user's computing device 14. In one embodiment of the present invention, the content server 22 freely releases and distributes packages 12p having digital content 12 to any distributes requesting same. However, the content server 22 may also release and distribute such packages 12p in a restricted manner without departing from the spirit and scope of the present invention. For example, the content server 22 may first require payment of a pre-determined distribution fee prior to distribution, or may require that a distributee identify itself, or may indeed make a determination of whether distribution is to occur based on an identification of the distributee.

[0086] In addition, the content server 22 may be employed to perform inventory management by controlling the authoring tool 18 to generate a number of different packages 12p in advance to meet an anticipated demand. For example, the server could generate 100 packages 12p based on the same digital content 12, and serve each package 12p 10 times. As supplies of packages 12p dwindle to 20, for example, the content server 22 may then direct the authoring tool 18 to generate 80 additional packages 12p, again for example.

[0087] Preferably, the content server 22 in the architecture 10 has a unique public private key pair (PU-CS, PR-CS) that is employed as part of the process of evaluating a license 16

and obtaining a decryption key (KD) for decrypting corresponding digital content 12, as will be explained in more detail below. As is known, a public/private key pair is an asymmetric key, in that what is encrypted in one of the keys in the key pair can only be decrypted by the other of the keys in the key pair. In a public/private key pair encryption system, the public key may be made known to the world, but the private key should always be held in confidence by the owner of such private key. Accordingly, if the content server 22 encrypts data with its private key (PR-CS), it can send the encrypted data out into the world with its public key (PU-CS) for decryption purposes. Correspondingly, if an external device wants to send data to the content server 22 so that only such content server 22 can decrypt such data, such external device must first obtain the public key of the content server 22 (PU-CS) and then must encrypt the data with such public key. Accordingly, the content server 22 (and only the content server 22) can then employ its private key (PR-CS) to decrypt such encrypted data.

[0088] As with the authoring tool 18, the content server 22 is implemented on an appropriate computer, processor, or other computing machine by way of appropriate software. The structure and operation of such machine and such software should be apparent based on the disclosure herein and therefore do not require any detailed discussion in the present disclosure. Moreover, in one embodiment of the present invention, the authoring tool 18 and the content server 22 may reside on a single computer, processor, or other computing machine, each in a separate work space. It should be recognized, moreover, that the content server 22 may in certain circumstances include the authoring tool 18 and/or perform the functions of the authoring tool 18, as discussed above.

[0089] Structure of Digital Content Package 12p

[0090] Referring now to FIG. 3, in one embodiment of the present invention, the digital content package 12p as distributed by the content server 22 includes:

[0091] the digital content 12 encrypted with the encryption/decryption key (KD), as was discussed above (i.e., (KD(CONTENT)));

[0092] the content ID (or package ID) of such digital content 12 (or package 12p);

[0093] the key ID of the decryption key (KD);

[0094] license acquisition information, preferably in an un-encrypted form; and

[0095] the key KD encrypting the content server 22 public key (PU-CS), signed by the content server 22 private key (PR-CS) (i.e., (KD (PU-CS) S (PR-CS))).

[0096] With regard to (KD (PU-CS) S (PR-CS)), it is to be understood that such item is to be used in connection with validating the digital content 12 and/or package 12p, as will be explained below. Unlike a certificate with a digital signature (see below), the key (PU-CS) is not necessary to get at (KD (PU-CS)). Instead, the key (PU-CS) is obtained merely by applying the decryption key (KD). Once so obtained, such key (PU-CS) may be employed to test the validity of the signature (S (PR-CS)).

[0097] It should also be understood that for such package 12p to be constructed by the authoring tool 18, such author-

ing tool 18 must already possess the license acquisition information and (KD (PU-CS) S (PR-CS)), presumably as header information supplied by the dictionary 28. Moreover, the authoring tool 18 and the content server 22 must presumably interact to construct (KD (PU-CS) S (PR-CS)). Such interaction may for example include the steps of:

- [0098] the content server 22 sending (PU-CS) to the authoring tool 18;
- [0099] the authoring tool 18 encrypting (PU-CS) with (KD) to produce (KD (PU-CS));
- [0100] the authoring tool 18 sending (KD (PU-CS)) to the content server 22;
- [0101] the content server 22 signing (KD (PU-CS)) with (PR-CS) to produce (KD (PU-CS) S (PR-CS)); and
- [0102] the content server 22 sending (KD (PU-CS) S (PR-CS)) to the authoring tool 18.

[0103] Architecture—License Server 24

[0104] Referring again to FIG. 1, in one embodiment of the present invention, the license server 24 performs the functions of receiving a request for a license 16 from a user's computing device 14 in connection with a piece of digital content 12, determining whether the user's computing device 14 can be trusted to honor an issued license 16, negotiating such a license 16, constructing such license 16, and transmitting such license 16 to the user's computing device 14. Preferably, such transmitted license 16 includes the decryption key (KD) for decrypting the digital content 12. Such license server 24 and such functions will be explained in more detail below. Preferably, and like the content server 22, the license server 24 in the architecture 10 has a unique public/private key pair (PU-LS, PR-LS) that is employed as part of the process of evaluating a license 16 and obtaining a decryption key (KD) for decrypting corresponding digital content 12, as will be explained in more detail below.

[0105] As with the authoring tool 18 and the content server 22, the license server 24 is implemented on an appropriate computer, processor, or other computing machine by way of appropriate software. The structure and operation of such machine and such software should be apparent based on the disclosure herein and therefore do not require any detailed discussion in the present disclosure. Moreover, in one embodiment of the present invention the authoring tool 18 and/or the content server 22 may reside on a single computer, processor, or other computing machine together with the license server 24, each in a separate work space.

[0106] In one embodiment of the present invention, prior to issuance of a license 16, the license server 24 and the content server 22 enter into an agency agreement or the like, wherein the license server 24 in effect agrees to be the licensing authority for at least a portion of the digital content 12 distributed by the content server 22. As should be understood, one content server 22 may enter into an agency agreement or the like with several license servers 24, and/or one license server 24 may enter into an agency agreement or the like with several content servers 22, all without departing from the spirit and scope of the present invention.

[0107] Preferably, the license server 24 can show to the world that it does in fact have the authority to issue a license 16 for digital content 12 distributed by the content server 22. To do so, it is preferable that the license server 24 send to the content server 22 the license server 24 public key (PU-LS), and that the content server 22 then send to the license server 24 a digital certificate containing PU-LS as the contents signed by the content server 22 private key (CERT (PU-LS) S (PR-CS)). As should be understood, the contents (PU-LS) in such certificate can only be accessed with the content server 22 public key (PU-CS). As should also be understood, in general, a digital signature of underlying data is an encrypted form of such data, and will not match such data when decrypted if such data has been adulterated or otherwise modified.

[0108] As a licensing authority in connection with a piece of digital content 12, and as part of the licensing function, the license server 24 must have access to the decryption key (KD) for such digital content 12. Accordingly, it is preferable that license server 24 have access to the content-key database 20 that has the decryption key (KD), key ID, and content ID (or package ID) for such digital content 12 (or package 12p).

[0109] Architecture—Black Box Server 26

[0110] Still referring to FIG. 1, in one embodiment of the present invention, the black box server 26 performs the functions of installing and/or upgrading a new black box 30 in a user's computing device 14. As will be explained in more detail below, the black box 30 performs encryption and decryption functions for the user's computing device 14. As will also be explained in more detail below, the black box 30 is intended to be secure and protected from attack. Such security and protection is provided, at least in part, by upgrading the black box 30 to a new version as necessary by way of the black box server 26, as will be explained in more detail below.

[0111] As with the authoring tool 18, the content server 22, and the license server 24, the black box server 26 is implemented on an appropriate computer, processor, or other computing machine by way of appropriate software. The structure and operation of such machine and such software should be apparent based on the disclosure herein and therefore do not require any detailed discussion in the present disclosure. Moreover, in one embodiment of the present invention the license server 24, the authoring tool 18, and/or the content server 22 may reside on a single computer, processor, or other computing machine together with the black box server 26, each in a separate work space. Note, though, that for security purposes, it may be wise to have the black box server 26 on a separate machine.

[0112] Architecture—User's Computing Device 14

[0113] Referring now to FIG. 4, in one embodiment of the present invention, the user's computing device 14 is a personal computer or the like, having elements including a keyboard, a mouse, a screen, a processor, RAM, ROM, a hard drive, a floppy drive, a CD player, and/or the like. However, the user's computing device 14 may also be a dedicated viewing device such as a television or monitor, a dedicated audio device such as a stereo or other music player, a dedicated printer, or the like, among other things, all without departing from the spirit and scope of the present invention.

[0114] The content owner for a piece of digital content 12 must trust that the user's computing device 14 will abide by the rules specified by such content owner, i.e. that the digital content 12 will not be rendered unless the user obtains a license 16 that permits the rendering in the manner sought. Preferably, then, the user's computing device 14 must provide a trusted component or mechanism 32 that can satisfy to the content owner that such computing device 14 will not render the digital content 12 except according to the license rules embodied in the license 16 associated with the digital content 12 and obtained by the user.

[0115] Here, the trusted mechanism 32 is a Digital Rights Management (DRM) system 32 that is enabled when a user requests that a piece of digital content 12 be rendered, that determines whether the user has a license 16 to render the digital content 12 in the manner sought, that effectuates obtaining such a license 16 if necessary, that determines whether the user has the right to play the digital content 12 according to the license 16, and that decrypts the digital content 12 for rendering purposes if in fact the user has such right according to such license 16. The contents and function of the DRM system 32 on the user's computing device 14 and in connection with the architecture 10 are described below.

[0116] DRM System 32

[0117] The DRM system 32 performs four main functions with the architecture 10 disclosed herein: (1) content acquisition, (2) license acquisition, (3) content rendering, and (4) black box 30 installation/update. Preferably, any of the functions can be performed at any time, although it is recognized that some of the functions already require that digital content 12 be acquired.

[0118] DRM System 32—Content Acquisition

[0119] Acquisition of digital content 12 by a user and/or the user's computing device 14 is typically a relatively straight-forward matter and generally involves placing a file having encrypted digital content 12 on the user's computing device 14. Of course, to work with the architecture 10 and the DRM system 32 disclosed herein, it is necessary that the encrypted digital content 12 be in a form that is amenable to such architecture 10 and DRM system 32, such as the digital package 12p as will be described below.

[0120] As should be understood, the digital content 12 may be obtained in any manner from a content server 22, either directly or indirectly, without departing from the spirit and scope of the present invention. For example, such digital content 12 may be downloaded from a network such as the Internet, located on an obtained optical or magnetic disk or the like, received as part of an E-mail message or the like, or downloaded from an electronic bulletin board or the like.

[0121] Such digital content 12, once obtained, is preferably stored in a manner such that the obtained digital content 12 is accessible by a rendering application 34 (to be described below) running on the computing device 14, and by the DRM system 32. For example, the digital content 12 may be placed as a file on a hard drive (not shown) of the user's computing device 14, or on a network server (not shown) accessible to the computing device 14. In the case where the digital content 12 is obtained on an optical or magnetic disk or the like, it may only be necessary that such

disk be present in an appropriate drive (not shown) coupled to the user's computing device 14.

[0122] In the present invention, it is not envisioned that any special tools are necessary to acquire digital content 12, either from the content server 22 as a direct distribution source or from some intermediary as an indirect distribution source. That is, it is preferable that digital content 12 be as easily acquired as any other data file. However, the DRM system 32 and/or the rendering application 34 may include an interface (not shown) designed to assist the user in obtaining digital content 12. For example, the interface may include a web browser especially designed to search for digital content 12, links to pre-defined Internet web sites that are known to be sources of digital content 12, and the like.

[0123] DRM System 32—Content Rendering, Part 1

[0124] Referring now to FIG. 5A, in one embodiment of the present invention, assuming the encrypted digital content 12 has been distributed to and received by a user and placed by the user on the computing device 14 in the form of a stored file, the user will attempt to render the digital content 12 by executing some variation on a render command (step 501). For example, such render command may be embodied as a request to 'play' or 'open' the digital content 12. In some computing environments, such as for example the "MICROSOFT WINDOWS" operating system, distributed by MICROSOFT Corporation of Redmond, Wash., such play or open command may be as simple as 'clicking' on an icon representative of the digital content 12. Of course, other embodiments of such render command may be employed without departing from the spirit and scope of the present invention. In general, such render command may be considered to be executed whenever a user directs that a file having digital content 12 be opened, run, executed, and/or the like.

[0125] Importantly, and in addition, such render command may be embodied as a request to copy the digital content 12 to another form, such as to a printed form, a visual form, an audio form, etc. As should be understood, the same digital content 12 may be rendered in one form, such as on a computer screen, and then in another form, such as a printed document. In the present invention, each type of rendering is performed only if the user has the right to do so, as will be explained below.

[0126] In one embodiment of the present invention, the digital content 12 is in the form of a digital file having a file name ending with an extension, and the computing device 14 can determine based on such extension to start a particular kind of rendering application 34. For example, if the file name extension indicates that the digital content 12 is a text file, the rendering application 34 is some form of word processor such as the "MICROSOFT WORD", distributed by MICROSOFT Corporation of Redmond, Washington. Likewise, if the file name extension indicates that the digital content 12 is an audio, video, and/or multimedia file, the rendering application 34 is some form of multimedia player, such as "MICROSOFT MEDIA PLAYER", also distributed by MICROSOFT Corporation of Redmond, Wash.

[0127] Of course, other methods of determining a rendering application may be employed without departing from the spirit and scope of the present invention. As but one example, the digital content 12 may contain meta-data in an

un-encrypted form (i.e., the aforementioned header information), where the meta-data includes information on the type of rendering application 34 necessary to render such digital content 12.

[0128] Preferably, such rendering application 34 examines the digital content 12 associated with the file name and determines whether such digital content 12 is encrypted in a rights-protected form (steps 503, 505). If not protected, the digital content 12 may be rendered without further ado (step 507). If protected, the rendering application 34 determines from the encrypted digital content 12 that the DRM system 32 is necessary to play such digital content 12. Accordingly, such rendering application 34 directs the user's computing device 14 to run the DRM system 32 thereon (step 509). Such rendering application 34 then calls such DRM system 32 to decrypt the digital content 12 (step 511). As will be discussed in more detail below, the DRM system 32 in fact decrypts the digital content 12 only if the user has a valid license 16 for such digital content 12 and the right to play the digital content 12 according to the license rules in the valid license 16. Preferably, once the DRM system 32 has been called by the rendering application 34, such DRM system 32 assumes control from the rendering application 34, at least for purposes of determining whether the user has a right to play such digital content 12 (step 513).

[0129] DRM System 32 Components

[0130] In one embodiment of the present invention, and referring again to FIG. 4, the DRM system 32 includes a license evaluator 36, the black box 30, a license store 38, and a state store 40.

[0131] DRM System 32 Components—License Evaluator 36

[0132] The license evaluator 36 locates one or more licenses 16 that correspond to the requested digital content 12, determines whether such licenses 16 are valid, reviews the license rules in such valid licenses 16, and determines based on the reviewed license rules whether the requesting user has the right to render the requested digital content 12 in the manner sought, among other things. As should be understood, the license evaluator 36 is a trusted component in the DRM system 32. In the present disclosure, to be 'trusted' means that the license server 24 (or any other trusting element) is satisfied that the trusted element will carry out the wishes of the owner of the digital content 12 according to the rights description in the license 16, and that a user cannot easily alter such trusted element for any purpose, nefarious or otherwise.

[0133] The license evaluator 36 has to be trusted in order to ensure that such license evaluator 36 will in fact evaluate a license 16 properly, and to ensure that such license evaluator 36 has not been adulterated or otherwise modified by a user for the purpose of bypassing actual evaluation of a license 16. Accordingly, the license evaluator 36 is run in a protected or shrouded environment such that the user is denied access to such license evaluator 36. Other protective measures may of course be employed in connection with the license evaluator 36 without departing from the spirit and scope of the present invention.

[0134] DRM System 32 Components—Black Box 30

[0135] Primarily, and as was discussed above, the black box 30 performs encryption and decryption functions in the

DRM system 32. In particular, the black box 30 works in conjunction with the license evaluator 36 to decrypt and encrypt certain information as part of the license evaluation function. In addition, once the license evaluator 36 determines that a user does in fact have the right to render the requested digital content 12 in the manner sought, the black box 30 is provided with a decryption key (KD) for such digital content 12, and performs the function of decrypting such digital content 12 based on such decryption key (KD).

[0136] The black box 30 is also a trusted component in the DRM system 32. In particular, the license server 24 must trust that the black box 30 will perform the decryption function only in accordance with the license rules in the license 16, and also trust that such black box 30 will not operate should it become adulterated or otherwise modified by a user for the nefarious purpose of bypassing actual evaluation of a license 16. Accordingly, the black box 30 is also run in a protected or shrouded environment such that the user is denied access to such black box 30. Again, other protective measures may be employed in connection with the black box 30 without departing from the spirit and scope of the present invention. Preferably, and like the content server 22 and license server 24, the black box 30 in the DRM system 32 has a unique public/private key pair (PU-BB, PR-BB) that is employed as part of the process of evaluating the license 16 and obtaining a decryption key (KD) for decrypting the digital content 12, as will be described in more detail below.

[0137] DRM System 32 Components—License Store 38

[0138] The license store 38 stores licenses 16 received by the DRM system 32 for corresponding digital content 12. The license store 38 itself need not be trusted since the license store 38 merely stores licenses 16, each of which already has trust components built thereinto, as will be described below. In one embodiment of the present invention, the license store 38 is merely a sub-directory of a drive such as a hard disk drive or a network drive. However, the license store 38 may be embodied in any other form without departing from the spirit and scope of the present invention, so long as such license store 38 performs the function of storing licenses 16 in a location relatively convenient to the DRM system 32.

[0139] DRM System 32 Components—State Store 40

[0140] The state store 40 performs the function of maintaining state information corresponding to licenses 16 presently or formerly in the license store 38. Such state information is created by the DRM system 32 and stored in the state store 40 as necessary. For example, if a particular license 16 only allows a pre-determined number of renderings of a piece of corresponding digital content 12, the state store 40 maintains state information on how many renderings have in fact taken place in connection with such license 16. The state store 40 continues to maintain state information on licenses 16 that are no longer in the license store 38 to avoid the situation where it would otherwise be advantageous to delete a license 16 from the license store 38 and then obtain an identical license 16 in an attempt to delete the corresponding state information from the state store 40.

[0141] The state store 40 also has to be trusted in order to ensure that the information stored therein is not reset to a state more favorable to a user. Accordingly, the state store 40

is likewise run in a protected or shrouded environment such that the user is denied access to such state store 40. Once again, other protective measures may of course be employed in connection with the state store 40 without departing from the spirit and scope of the present invention. For example, the state store 40 may be stored by the DRM system 32 on the computing device 14 in an encrypted form.

[0142] DRM System 32—Content Rendering, Part 2

[0143] Referring again to FIG. 5A, and again discussing content rendering in one embodiment of the present invention, once the DRM system 32 has assumed control from the calling rendering application 34, such DRM system 32 then begins the process of determining whether the user has a right to render the requested digital content 12 in the manner sought. In particular, the DRM system 32 either locates a valid, enabling license 16 in the license store (steps 515, 517) or attempts to acquire a valid, enabling license 16 from the license server 24 (i.e. performs the license acquisition function as discussed below and as shown in FIG. 7).

[0144] As a first step, and referring now to FIG. 6, the license evaluator 36 of such DRM system 32 checks the license store 38 for the presence of one or more received licenses 16 that correspond to the digital content 12 (step 601). Typically, the license 16 is in the form of a digital file, as will be discussed below, although it will be recognized that the license 16 may also be in other forms without departing from the spirit and scope of the present invention. Typically, the user will receive the digital content 12 without such license 16, although it will likewise be recognized that the digital content 12 may be received with a corresponding license 16 without departing from the spirit and scope of the present invention.

[0145] As was discussed above in connection with FIG. 3, each piece of digital content 12 is in a package 12p with a content ID (or package ID) identifying such digital content 12 (or package 12p), and a key ID identifying the decryption key (KD) that will decrypt the encrypted digital content 12. Preferably, the content ID (or package ID) and the key ID are in an un-encrypted form. Accordingly, and in particular, based on the content ID of the digital content 12, the license evaluator 36 looks for any license 16 in the license store 38 that contains an identification of applicability to such content ID. Note that multiple such licenses 16 may be found, especially if the owner of the digital content 12 has specified several different kinds of licenses 16 for such digital content 12, and the user has obtained multiple ones of such licenses 16. If in fact the license evaluator 36 does not find in the license store 38 any license 16 corresponding to the requested digital content 12, the DRM system 32 may then perform the function of license acquisition (step 519 of FIG. 5), to be described below.

[0146] Assume now that the DRM system 32 has been requested to render a piece of digital content 12, and one or more licenses 16 corresponding thereto are present in the license store 38. In one embodiment of the present invention, then, the license evaluator 36 of the DRM system 32 proceeds to determine for each such license 16 whether such license 16 itself is valid (steps 603 and 605 of FIG. 6). Preferably, and in particular, each license 16 includes a digital signature 26 based on the content 28 of the license 16. As should be understood, the digital signature 26 will not match the license 16 if the content 28 has been adulterated

or otherwise modified. Thus, the license evaluator 36 can determine based on the digital signature 26 whether the content 28 is in the form that it was received from the license server 24 (i.e., is valid). If no valid license 16 is found in the license store 38, the DRM system 32 may then perform the license acquisition function described below to obtain such a valid license 16.

[0147] Assuming that one or more valid licenses 16 are found, for each valid license 16, the license evaluator 36 of the DRM system 32 next determines whether such valid license 16 gives the user the right to render the corresponding digital content 12 in the manner desired (i.e., is enabling) (steps 607 and 609). In particular, the license evaluator 36 determines whether the requesting user has the right to play the requested digital content 12 based on the rights description in each license 16 and based on what the user is attempting to do with the digital content 12. For example, such rights description may allow the user to render the digital content 12 into a sound, but not into a decrypted digital copy.

[0148] As should be understood, the rights description in each license 16 specifies whether the user has rights to play the digital content 12 based on any of several factors, including who the user is, where the user is located, what type of computing device 14 the user is using, what rendering application 34 is calling the DRM system 32, the date, the time, etc. In addition, the rights description may limit the license 16 to a pre-determined number of plays, or pre-determined play time, for example. In such case, the DRM system 32 must refer to any state information with regard to the license 16, (i.e., how many times the digital content 12 has been rendered, the total amount of time the digital content 12 has been rendered, etc.), where such state information is stored in the state store 40 of the DRM system 32 on the user's computing device 14.

[0149] Accordingly, the license evaluator 36 of the DRM system 32 reviews the rights description of each valid license 16 to determine whether such valid license 16 confers the rights sought to the user. In doing so, the license evaluator 36 may have to refer to other data local to the user's computing device 14 to perform a determination of whether the user has the rights sought. As seen in FIG. 4, such data may include an identification 42 of the user's computing device (machine) 14 and particular aspects thereof, an identification 44 of the user and particular aspects thereof, an identification of the rendering application 34 and particular aspects thereof, a system clock 46, and the like. If no valid license 16 is found that provides the user with the right to render the digital content 12 in the manner sought, the DRM system 32 may then perform the license acquisition function described below to obtain such a license 16, if in fact such a license 16 is obtainable.

[0150] Of course, in some instances the user cannot obtain the right to render the digital content 12 in the manner requested, because the content owner of such digital content 12 has in effect directed that such right not be granted. For example, the content owner of such digital content 12 may have directed that no license 16 be granted to allow a user to print a text document, or to copy a multimedia presentation into an un-encrypted form. In one embodiment of the present invention, the digital content 12 includes data on what rights are available upon purchase of a license 16, and

types of licenses 16 available. However, it will be recognized that the content owner of a piece of digital content 12 may at any time change the rights currently available for such digital content 12 by changing the licenses 16 available for such digital content 12.

[0151] DRM System 32—License Acquisition

[0152] Referring now to FIG. 7, if in fact the license evaluator 36 does not find in the license store 38 any valid, enabling license 16 corresponding to the requested digital content 12, the DRM system 32 may then perform the function of license acquisition. As shown in FIG. 3, each piece of digital content 12 is packaged with information in an un-encrypted form regarding how to obtain a license 16 for rendering such digital content 12 (i.e., license acquisition information).

[0153] In one embodiment of the present invention, such license acquisition information may include (among other things) types of licenses 16 available, and one or more Internet web sites or other site information at which one or more appropriate license servers 24 may be accessed, where each such license server 24 is in fact capable of issuing a license 16 corresponding to the digital content 12. Of course, the license 16 may be obtained in other manners without departing from the spirit and scope of the present invention. For example, the license 16 may be obtained from a license server 24 at an electronic bulletin board, or even in person or via regular mail in the form of a file on a magnetic or optical disk or the like.

[0154] Assuming that the location for obtaining a license 16 is in fact a license server 24 on a network, the license evaluator 36 then establishes a network connection to such license server 24 based on the web site or other site information, and then sends a request for a license 16 from such connected license server 24 (steps 701, 703). In particular, once the DRM system 32 has contacted the license server 24, such DRM system 32 transmits appropriate license request information 36 to such license server 24. In one embodiment of the present invention, such license 16 request information 36 may include:

[0155] the public key of the black box 30 of the DRM system 32 (PU-BB);

[0156] the version number of the black box 30 of the DRM system 32;

[0157] a certificate with a digital signature from a certifying authority certifying the black box 30 (where the certificate may in fact include the aforementioned public key and version number of the black box 30);

[0158] the content ID (or package ID) that identifies the digital content 12 (or package 12p);

[0159] the key ID that identifies the decryption key (KD) for decrypting the digital content 12;

[0160] the type of license 16 requested (if in fact multiple types are available);

[0161] the type of rendering application 34 that requested rendering of the digital content 12;

[0162] and/or the like, among other things. Of course, greater or lessor amounts of license 16 request information

36 may be transmitted to the license server 24 by the DRM system 32 without departing from the spirit and scope of the present invention. For example, information on the type of rendering application 34 may not be necessary, while additional information about the user and/or the user's computing device 14 may be necessary.

[0163] Once the license server 24 has received the license 16 request information 36 from the DRM system 32, the license server 24 may then perform several checks for trust/authentication and for other purposes. In one embodiment of the present invention, such license server 24 checks the certificate with the digital signature of the certifying authority to determine whether such has been adulterated or otherwise modified (steps 705, 707). If so, the license server 24 refuses to grant any license 16 based on the request information 36. The license server 24 may also maintain a list of known 'bad' users and/or user's computing devices 14, and may refuse to grant any license 16 based on a request from any such bad user and/or bad user's computing device 14 on the list. Such 'bad' list may be compiled in any appropriate manner without departing from the spirit and scope of the present invention.

[0164] Based on the received request and the information associated therewith, and particularly based on the content ID (or package ID) in the license request information, the license server 24 can interrogate the content-key database 20 (FIG. 1) and locate a record corresponding to the digital content 12 (or package 12p) that is the basis of the request. As was discussed above, such record contains the decryption key (KD), key ID, and content ID for such digital content 12. In addition, such record may contain license data regarding the types of licenses 16 to be issued for the digital content 12 and the terms and conditions for each type of license 16. Alternatively, such record may include a pointer, link, or reference to a location having such additional information.

[0165] As mentioned above, multiple types of licenses 16 may be available. For example, for a relatively small license fee, a license 16 allowing a limited number of renderings may be available. For a relatively greater license fee, a license 16 allowing unlimited renderings until an expiration date may be available. For a still greater license fee, a license 16 allowing unlimited renderings without any expiration date may be available. Practically any type of license 16 having any kind of license terms may be devised and issued by the license server 24 without departing from the spirit and scope of the present invention.

[0166] In one embodiment of the present invention, the request for a license 16 is accomplished with the aid of a web page or the like as transmitted from the license server 24 to the user's computing device 14. Preferably, such web page includes information on all types of licenses 16 available from the license server 24 for the digital content 12 that is the basis of the license 16 request.

[0167] In one embodiment of the present invention, prior to issuing a license 16, the license server 24 checks the version number of the black box 30 to determine whether such black box 30 is relatively current (steps 709, 711). As should be understood, the black box 30 is intended to be secure and protected from attacks from a user with nefarious purposes (i.e., to improperly render digital content 12 without a license 16, or outside the terms of a corresponding

license 16). However, it is to be recognized that no system and no software device is in fact totally secure from such an attack.

[0168] As should also be understood, if the black box 30 is relatively current, i.e., has been obtained or updated relatively recently, it is less likely that such black box 30 has been successfully attacked by such a nefarious user. Preferably, and as a matter of trust, if the license server 24 receives a license request with request information 36 including a black box 30 version number that is not relatively current, such license server 24 refuses to issue the requested license 16 until the corresponding black box 30 is upgraded to a current version, as will be described below. Put simply, the license server 24 will not trust such black box 30 unless such black box 30 is relatively current.

[0169] In the context of the black box 30 of the present invention, the term 'current' or 'relatively current' may have any appropriate meaning without departing from the spirit and scope of the present invention, consistent with the function of providing trust in the black box 30 based on the age or use thereof. For example, 'current' may be defined according to age (i.e., less than one month old). As an alternative example, 'current' may be defined based on a number of times that the black box 30 has decrypted digital content 12 (i.e., less than 200 instances of decryption). Moreover, 'current' may be based on policy as set by each license server 24, where one license server 24 may define 'current' differently from another license server 24, and a license server 24 may further define 'current' differently depending on the digital content 12 for which a license 16 is requested, or depending on the type of license 16 requested, among other things.

[0170] Assuming that the license server 24 is satisfied from the version number of a black box 30 or other indicia thereof that such black box 30 is current, the license server 24 then proceeds to negotiate terms and conditions for the license 16 with the user (step 713). Alternatively, the license server 24 negotiates the license 16 with the user, then satisfies itself from the version number of the black box 30 that such black box 30 is current (i.e., performs step 713, then step 711). Of course, the amount of negotiation varies depending on the type of license 16 to be issued, and other factors. For example, if the license server 24 is merely issuing a paid-up unlimited use license 16, very little need be negotiated. On the other hand, if the license 16 is to be based on such items as varying values, sliding scales, break points, and other details, such items and details may need to be worked out between the license server 24 and the user before the license 16 can be issued.

[0171] As should be understood, depending on the circumstances, the license negotiation may require that the user provide further information to the license server 24 (for example, information on the user, the user's computing device 14, etc.). Importantly, the license negotiation may also require that the user and the license server 24 determine a mutually acceptable payment instrument (a credit account, a debit account, a mailed check, etc.) and/or payment method (paid-up immediately, spread over a period of time, etc.), among other things.

[0172] Once all the terms of the license 16 have been negotiated and agreed to by both the license server 24 and user (step 715), a digital license 16 is generated by the

license server 24 (step 719), where such generated license 16 is based at least in part on the license request, the black box 30 public key (PU-BB), and the decryption key (KD) for the digital content 12 that is the basis of the request as obtained from the content-key database 20. In one embodiment of the present invention, and as seen in FIG. 8, the generated license 16 includes:

[0173] the content ID of the digital content 12 to which the license 16 applies;

[0174] a Digital Rights License (DRL) 48 (i.e., the rights description or actual terms and conditions of the license 16 written in a predetermined form that the license evaluator 36 can interrogate), perhaps encrypted with the decryption key (KD) (i.e., KD (DRL));

[0175] the decryption key (KD) for the digital content 12 encrypted with the black box 30 public key (PU-BB) as received in the license request (i.e., (PU-BB (KD)));

[0176] a digital signature from the license server 24 (without any attached certificate) based on (KD (DRL)) and (PU-BB (KD)) and encrypted with the license server 24 private key (i.e., (S (PR-LS))); and

[0177] the certificate that the license server 24 obtained previously from the content server 22, such certificate indicating that the license server 24 has the authority from the content server 22 to issue the license 16 (i.e., (CERT (PU-LS) S (PR-CS))).

[0178] As should be understood, the aforementioned elements and perhaps others are packaged into a digital file or some other appropriate form. As should also be understood, if the DRL 48 or (PU-BB (KD)) in the license 16 should become adulterated or otherwise modified, the digital signature (S (PR-LS)) in the license 16 will not match and therefore will not validate such license 16. For this reason, the DRL 48 need not necessarily be in an encrypted form (i.e., (KD(DRL)) as mentioned above), although such encrypted form may in some instances be desirable and therefore may be employed without departing from the spirit and scope of the present invention.

[0179] Once the digital license 16 has been prepared, such license 16 is then issued to the requestor (i.e., the DRM system 32 on the user's computing device 14) (step 719 of FIG. 7). Preferably, the license 16 is transmitted over the same path through which the request therefor was made (i.e., the Internet or another network), although another path may be employed without departing from the spirit and scope of the present invention. Upon receipt, the requesting DRM system 32 preferably automatically places the received digital license 16 in the license store 38 (step 721).

[0180] It is to be understood that a user's computing device 14 may on occasion malfunction, and licenses 16 stored in the license store 38 of the DRM system 32 on such user's computing device 14 may become irretrievably lost. Accordingly, it is preferable that the license server 24 maintain a database 50 of issued licenses 16 (FIG. 1), and that such license server 24 provide a user with a copy or re-issue (hereinafter 're-issue') of an issued license 16 if the user is in fact entitled to such re-issue. In the aforementioned case where licenses 16 are irretrievably lost, it is also likely

the case that state information stored in the state store 40 and corresponding to such licenses 16 is also lost. Such lost state information should be taken into account when re-issuing a license 16. For example, a fixed number of renderings license 16 might legitimately be re-issued in a pro-rated form after a relatively short period of time, and not re-issued at all after a relatively longer period of time.

[0181] DRM System 32—Installation/Upgrade of Black Box 30

[0182] As was discussed above, as part of the function of acquiring a license 16, the license server 24 may deny a request for a license 16 from a user if the user's computing device 14 has a DRM system 32 with a black box 30 that is not relatively current, i.e., has a relatively old version number. In such case, it is preferable that the black box 30 of such DRM system 32 be upgraded so that the license acquisition function can then proceed. Of course, the black box 30 may be upgraded at other times without departing from the spirit and scope of the present invention.

[0183] Preferably, as part of the process of installing the DRM system 32 on a user's computing device 14, a non-unique 'lite' version of a black box 30 is provided. Such 'lite' black box 30 is then upgraded to a unique regular version prior to rendering a piece of digital content 12. As should be understood, if each black box 30 in each DRM system 32 is unique, a security breach into one black box 30 cannot easily be replicated with any other black box 30.

[0184] Referring now to FIG. 9, the DRM system 32 obtains the unique black box 30 by requesting same from a black box server 26 or the like (as was discussed above and as shown in FIG. 1) (step 901). Typically, such request is made by way of the Internet, although other means of access may be employed without departing from the spirit and scope of the present invention. For example, the connection to a black box server 26 may be a direct connection, either locally or remotely. An upgrade from one unique non-lite black box 30 to another unique non-lite black box 30 may also be requested by the DRM system 32 at any time, such as for example a time when a license server 24 deems the black box 30 not current, as was discussed above.

[0185] Thereafter, the black box server 26 generates a new unique black box 30 (step 903). As seen in FIG. 3, each new black box 30 is provided with a version number and a certificate with a digital signature from a certifying authority. As was discussed above in connection with the license acquisition function, the version number of the black box 30 indicates the relative age and/or use thereof. The certificate with the digital signature from the certifying authority, also discussed above in connection with the license acquisition function, is a proffer or vouching mechanism from the certifying authority that a license server 24 should trust the black box 30. Of course, the license server 24 must trust the certifying authority to issue such a certificate for a black box 30 that is in fact trustworthy. It may be the case, in fact, that the license server 24 does not trust a particular certifying authority, and refuses to honor any certificate issued by such certifying authority. Trust may not occur, for example, if a particular certifying authority is found to be engaging in a pattern of improperly issuing certificates.

[0186] Preferably, and as was discussed above, the black box server 26 includes a new unique public/private key pair

(PU-BB, PR-BB) with the newly generated unique black box 30 (step 903 of FIG. 9). Preferably, the private key for the black box 30 (PR-BB) is accessible only to such black box 30, and is hidden from and inaccessible by the remainder of the world, including the computing device 14 having the DRM system 32 with such black box 30, and the user thereof.

[0187] Most any hiding scheme may be employed without departing from the spirit and scope of the present invention, so long as such hiding scheme in fact performs the function of hiding the private key (PR-BB) from the world. As but one example, the private key (PR-BB) may be split into several sub-components, and each sub-component may be encrypted uniquely and stored in a different location. In such a situation, it is preferable that such sub-components are never assembled in full to produce the entire private key (PR-BB).

[0188] In one embodiment of the present invention, such private key (PR-BB) is encrypted according to code-based encryption techniques. In particular, in such embodiment, the actual software code of the black box 30 (or other software code) is employed as encrypting key(s). Accordingly, if the code of the black box 30 (or the other software code) becomes adulterated or otherwise modified, for example by a user with nefarious purposes, such private key (PR-BB) cannot be decrypted.

[0189] Although each new black box 30 is delivered with a new public/private key pair (PU-BB, PR-BB), such new black box 30 is also preferably given access to old public/private key pairs from old black boxes 30 previously delivered to the DRM system 32 on the user's computing device 14 (step 905). Accordingly, the upgraded black box 30 can still employ the old key pairs to access older digital content 12 and older corresponding licenses 16 that were generated according to such old key pairs, as will be discussed in more detail below.

[0190] Preferably, the upgraded black box 30 delivered by the black box server 26 is tightly tied to or associated with the user's computing device 14. Accordingly, the upgraded black box 30 cannot be operably transferred among multiple computing devices 14 for nefarious purposes or otherwise. In one embodiment of the present invention, as part of the request for the black box 30 (step 901) the DRM system 32 provides hardware information unique to such DRM system 32 and/or unique to the user's computing device 14 to the black box server 26, and the black box server 26 generates a black box 30 for the DRM system 32 based in part on such provided hardware information. Such generated upgraded black box 30 is then delivered to and installed in the DRM system 32 on the user's computing device 14 (steps 907, 909). If the upgraded black box 30 is then somehow transferred to another computing device 14, the transferred black box 30 recognizes that it is not intended for such other computing device 14, and does not allow any requested rendering to proceed on such other computing device 14.

[0191] Once the new black box 30 is installed in the DRM system 32, such DRM system 32 can proceed with a license acquisition function or with any other function.

[0192] DRM System 32—Content Rendering, Part 3

[0193] Referring now to FIG. 5B, and assuming, now, that the license evaluator 36 has found at least one valid license

16 and that at least one of such valid licenses **16** provides the user with the rights necessary to render the corresponding digital content **12** in the manner sought (i.e., is enabling), the license evaluator **36** then selects one of such licenses **16** for further use (step **519**). Specifically, to render the requested digital content **12**, the license evaluator **36** and the black box **30** in combination obtain the decryption key (KD) from such license **16**, and the black box **30** employs such decryption key (KD) to decrypt the digital content **12**. In one embodiment of the present invention, and as was discussed above, the decryption key (KD) as obtained from the license **16** is encrypted with the black box **30** public key (PU-BB(KD)), and the black box **30** decrypts such encrypted decryption key with its private key (PR-BB) to produce the decryption key (KD) (steps **521**, **523**). However, other methods of obtaining the decryption key (KD) for the digital content **12** may be employed without departing from the spirit and scope of the present invention.

[0194] Once the black box **30** has the decryption key (KD) for the digital content **12** and permission from the license evaluator **36** to render the digital content **12**, control may be returned to the rendering application **34** (steps **525**, **527**). In one embodiment of the present invention, the rendering application **34** then calls the DRM system **32**/black box **30** and directs at least a portion of the encrypted digital content **12** to the black box **30** for decryption according to the decryption key (KD) (step **529**). The black box **30** decrypts the digital content **12** based upon the decryption key (KD) for the digital content **12**, and then the black box **30** returns the decrypted digital content **12** to the rendering application **34** for actual rendering (steps **533**, **535**). The rendering application **34** may either send a portion of the encrypted digital content **12** or the entire digital content **12** to the black box **30** for decryption based on the decryption key (KD) for such digital content **12** without departing from the spirit and scope of the present invention.

[0195] Preferably, when the rendering application **34** sends digital content **12** to the black box **30** for decryption, the black box **30** and/or the DRM system **32** authenticates such rendering application **34** to ensure that it is in fact the same rendering application **34** that initially requested the DRM system **32** to run (step **531**). Otherwise, the potential exists that rendering approval may be obtained improperly by basing the rendering request on one type of rendering application **34** and in fact rendering with another type of rendering application **34**. Assuming the authentication is successful and the digital content **12** is decrypted by the black box **30**, the rendering application **34** may then render the decrypted digital content **12** (steps **533**, **535**).

[0196] Sequence of Key Transactions

[0197] Referring now to FIG. 10, in one embodiment of the present invention, a sequence of key transactions is performed to obtain the decryption key (KD) and evaluate a license **16** for a requested piece of digital content **12** (i.e., to perform steps **515**-**523** of FIGS. **5A** and **5B**). Mainly, in such sequence, the DRM system **32** obtains the decryption key (KD) from the license **16**, uses information obtained from the license **16** and the digital content **12** to authenticate or ensure the validity of both, and then determines whether the license **16** in fact provides the right to render the digital content **12** in the manner sought. If so, the digital content **12** may be rendered.

[0198] Bearing in mind that each license **16** for the digital content **12**, as seen in FIG. 8, includes:

[0199] the content ID of the digital content **12** to which the license **16** applies;

[0200] the Digital Rights License (DRL) **48**, perhaps encrypted with the decryption key (KD) (i.e., KD(DRL));

[0201] the decryption key (KD) for the digital content **12** encrypted with the black box **30** public key (PU-BB) (i.e., (PU-BB (KD)));

[0202] the digital signature from the license server **24** based on (KD (DRL)) and (PU-BB (KD)) and encrypted with the license server **24** private key (i.e., (S (PR-LS))); and

[0203] the certificate that the license server **24** obtained previously from the content server **22** (i.e., (CERT (PU-CS) S (PR-CS))),

[0204] and also bearing in mind that the package **12p** having the digital content **12**, as seen in FIG. 3, includes:

[0205] the content ID of such digital content **12**;

[0206] the digital content **12** encrypted by KD (i.e., (KD(CONTENT)));

[0207] a license acquisition script that is not encrypted; and

[0208] the key KD encrypting the content server **22** public key (PU-CS), signed by the content server **22** private key (PR-CS) (i.e., (KD (PU-CS) S (PR-CS))),

[0209] in one embodiment of the present invention, the specific sequence of key transactions that are performed with regard to a specific one of the licenses **16** for the digital content **12** is as follows:

[0210] 1. Based on (PU-BB (KD)) from the license **16**, the black box **30** of the DRM system **32** on the user's computing device **14** applies its private key (PR-BB) to obtain (KD) (step **1001**). (PR-BB (PU-BB (KD))=(KD)). Note, importantly, that the black box **30** could then proceed to employ KD to decrypt the digital content **12** without any further ado. However, and also importantly, the license server **24** trusts the black box **30** not to do so. Such trust was established at the time such license server **24** issued the license **16** based on the certificate from the certifying authority vouching for the trustworthiness of such black box **30**. Accordingly, despite the black box **30** obtaining the decryption key (KD) as an initial step rather than a final step, the DRM system **32** continues to perform all license **16** validation and evaluation functions, as described below.

[0211] 2. Based on (KD (PU-CS) S (PR-CS)) from the digital content **12**, the black box **30** applies the newly obtained decryption key (KD) to obtain (PU-CS) (step **1003**). (KD (KD (PU-CS))=(PU-CS)). Additionally, the black box **30** can apply (PU-CS) as against the signature (S (PR-CS)) to satisfy itself that such signature and such digital content **12**/package **12p** is valid

(step 1005). If not valid, the process is halted and access to the digital content 12 is denied.

[0212] 3. Based on (CERT (PU-LS) S (PR-CS)) from the license 16, the black box 30 applies the newly obtained content server 22 public key (PU-CS) to satisfy itself that the certificate is valid (step 1007), signifying that the license server 24 that issued the license 16 had the authority from the content server 22 to do so, and then examines the certificate contents to obtain (PU-LS) (step 1009). If not valid, the process is halted and access to the digital content 12 based on the license 16 is denied.

[0213] 4. Based on (S (PR-LS)) from the license 16, the black box 30 applies the newly obtained license server 24 public key (PU-LS) to satisfy itself that the license 16 is valid (step 1011). If not valid, the process is halted and access to the digital content 12 based on the license 16 is denied.

[0214] 5. Assuming all validation steps are successful, and that the DRL 48 in the license 16 is in fact encrypted with the decryption key (KD), the license evaluator 36 then applies the already-obtained decryption key (KD) to (KD(DRL)) as obtained from the license 16 to obtain the license terms from the license 16 (i.e., the DRL 48) (step 1013). Of course, if the DRL 48 in the license 16 is not in fact encrypted with the decryption key (KD), step 1013 may be omitted. The license evaluator 36 then evaluates/interrogates the DRL 48 and determines whether the user's computing device 14 has the right based on the DRL 48 in the license 16 to render the corresponding digital content 12 in the manner sought (i.e., whether the DRL 48 is enabling) (step 1015). If the license evaluator 36 determines that such right does not exist, the process is halted and access to the digital content 12 based on the license 16 is denied.

[0215] 6. Finally, assuming evaluation of the license 16 results in a positive determination that the user's computing device 14 has the right based on the DRL 48 terms to render the corresponding digital content 12 in the manner sought, the license evaluator 36 informs the black box 30 that such black box 30 can render the corresponding digital content 12 according to the decryption key (KD). The black box 30 thereafter applies the decryption key (KD) to decrypt the digital content 12 from the package 12p (i.e., (KD(KD(CONTENT))=(CONTENT))) (step 1017).

[0216] It is important to note that the above-specified series of steps represents an alternating or 'ping-ponging' between the license 16 and the digital content 12. Such ping-ponging ensures that the digital content 12 is tightly bound to the license 16, in that the validation and evaluation process can only occur if both the digital content 12 and license 16 are present in a properly issued and valid form. In addition, since the same decryption key (KD) is needed to get the content server 22 public key (PU-CS) from the license 16 and the digital content 12 from the package 12p in a decrypted form (and perhaps the license terms (DRL 48) from the license 16 in a decrypted form), such items are also tightly bound. Signature validation also ensures that the digital content 12 and the license 16 are in the same form as issued from the content server 22 and the license server 24,

respectively. Accordingly, it is difficult if not impossible to decrypt the digital content 12 by bypassing the license server 24, and also difficult if not impossible to alter and then decrypt the digital content 12 or the license 16.

[0217] In one embodiment of the present invention, signature verification, and especially signature verification of the license 16, is alternately performed as follows. Rather than having a signature encrypted by the private key of the license server 16 (PR-LS), as is seen in FIG. 8, each license 16 has a signature encrypted by a private root key (PR-R) (not shown), where the black box 30 of each DRM system 32 includes a public root key (PU-R) (also not shown) corresponding to the private root key (PR-R). The private root key (PR-R) is known only to a root entity, and a license server 24 can only issue licenses 16 if such license server 24 has arranged with the root entity to issue licenses 16.

[0218] In particular, in such embodiment:

[0219] 1. the license server 24 provides its public key (PU-LS) to the root entity;

[0220] 2. the root entity returns the license server public key (PU-LS) to such license server 24 encrypted with the private root key (PR-R) (i.e., (CERT (PU-LS) S (PR-R))); and

[0221] 3. the license server 24 then issues a license 16 with a signature encrypted with the license server private key (S(PR-LS)), and also attaches to the license the certificate from the root entity (CERT (PU-LS) S (PR-R)).

[0222] For a DRM system 18 to validate such issued license 16, then, the DRM system 18:

[0223] 1. applies the public root key (PU-R) to the attached certificate (CERT (PU-LS) S (PR-R)) to obtain the license server public key (PU-LS); and

[0224] 2. applies the obtained license server public key (PU-LS) to the signature of the license 16 (S (PR-LS)).

[0225] Importantly, it should be recognized that just as the root entity gave the license server 24 permission to issue licenses 16 by providing the certificate (CERT (PU-LS) S (PR-R)) to such license server 24, such license server 24 can provide a similar certificate to a second license server 24 (i.e., (CERT (PU-LS2) S (PR-LS1))), thereby allowing the second license server to also issue licenses 16. As should now be evident, a license 16 issued by the second license server would include a first certificate (CERT (PU-LS1) S (PR-R)) and a second certificate (CERT (PU-LS2) S (PR-LS1)). Likewise, such license 16 is validated by following the chain through the first and second certificates. Of course, additional links in the chain may be added and traversed.

[0226] One advantage of the aforementioned signature verification process is that the root entity may periodically change the private root key (PR-R), thereby likewise periodically requiring each license server 24 to obtain a new certificate (CERT (PU-LS) S (PR-R)). Importantly, as a requirement for obtaining such new certificate, each license server may be required to upgrade itself. As with the black box 30, if a license server 24 is relatively current, i.e., has been upgraded relatively recently, it is less likely that license server 24 has been successfully attacked. Accordingly, as a matter of trust, each license server 24 is preferably required

to be upgraded periodically via an appropriate upgrade trigger mechanism such as the signature verification process. Of course, other upgrade mechanisms may be employed without departing from the spirit and scope of the present invention.

[0227] Of course, if the private root key (PR-R) is changed, then the public root key (PU-R) in each DRM system 18 must also be changed. Such change may for example take place during a normal black box 30 upgrade, or in fact may require that a black box 30 upgrade take place. Although a changed public root key (PU-R) may potentially interfere with signature validation for an older license 16 issued based on an older private root key (PR-R), such interference may be minimized by requiring that an upgraded black box 30 remember all old public root keys (PU-R). Alternatively, such interference may be minimized by requiring signature verification for a license 16 only once, for example the first time such license 16 is evaluated by the license evaluator 36 of a DRM system 18. In such case, state information on whether signature verification has taken place should be compiled, and such state information should be stored in the state store 40 of the DRM system 18.

[0228] Digital Rights License 48

[0229] In one embodiment of the present invention, the license evaluator 36 evaluates a Digital Rights License (DRL) 48 as the rights description or terms of a license 16 to determine if such DRL 48 allows rendering of a corresponding piece of digital content 12 in the manner sought. In one embodiment of the present invention, the DRL 48 may be written by a licensor (i.e., the content owner) in any DRL language.

[0230] As should be understood, there are a multitude of ways to specify a DRL 48. Accordingly, a high degree of flexibility must be allowed for in any DRL language. However, it is impractical to specify all aspects of a DRL 48 in a particular license language, and it is highly unlikely that the author of such a language can appreciate all possible licensing aspects that a particular digital licensor may desire. Moreover, a highly sophisticated license language may be unnecessary and even hindrance for a licensor providing a relatively simple DRL 48. Nevertheless, a licensor should not be unnecessarily restricted in how to specify a DRL 48. At the same time, the license evaluator 36 should always be able to get answers from a DRL 48 regarding a number of specific license questions.

[0231] In the present invention, and referring now to FIG. 11, a DRL 48 can be specified in any license language, but includes a language identifier or tag 54. The license evaluator 36 evaluating the license 16, then, performs the preliminary step of reviewing the language tag 54 to identify such language, and then selects an appropriate license language engine 52 for accessing the license 16 in such identified language. As should be understood, such license language engine 52 must be present and accessible to the license evaluator 36. If not present, the language tag 54 and/or the DRL 48 preferably includes a location 56 (typically a web site) for obtaining such language engine 52.

[0232] Typically, the language engine 52 is in the form of an executable file or set of files that reside in a memory of the user's computing device 14, such as a hard drive. The language engine 52 assists the license evaluator 36 to directly interrogate the DRL 48, the license evaluator 36 interrogates the DRL 48 indirectly via the language engine 48 acting as an intermediary, or the like. When executed, the language engine 52 runs in a work space in a memory of the user's computing device 14, such as RAM. However, any other form of language engine 52 may be employed without departing from the spirit and scope of the present invention.

[0233] Preferably, any language engine 52 and any DRL language supports at least a number of specific license questions that the license evaluator 36 expects to be answered by any DRL 48, as will be discussed below. Accordingly, the license evaluator 36 is not tied to any particular DRL language; a DRL 48 may be written in any appropriate DRL language; and a DRL 48 specified in a new license language can be employed by an existing license evaluator 36 by having such license evaluator 36 obtain a corresponding new language engine 52.

[0234] DRL Languages

[0235] Two examples of DRL languages, as embodied in respective DRLs 48, are provided below. The first, 'simple' DRL 48 is written in a DRL language that specifies license attributes, while the second 'script' DRL 48 is written in a DRL language that can perform functions according to the script specified in the DRL 48. While written in a DRL language, the meaning of each line of code should be apparent based on the linguistics thereof and/or on the attribute description chart that follows:

Simple DRL 48:

```
<LICENSE>
<DATA>
<NAME>Beastie Boy's Play</NAME>
<ID>39384</ID>
<DESCRIPTION>Play the song 3 times</DESCRIPTION>
<TERMS></TERMS>
<VALIDITY>
<NOTBEFORE>19980102 23:20:14Z</NOTBEFORE>
<NOTAFTER>19980102 23:20:14Z</NOTAFTER>
<VALIDITY>
<ISSUEDATE>19980102 23:20:14Z</ISSUEDATE>
<LICENSORSITE>http://www.foo.com</LICENSORSITE>
<CONTENT>
<NAME>Beastie Boy's</NAME>
```

-continued

```

<ID>392</ID>
<KEYID>39292</KEYID>
<TYPE>MS Encrypted ASF 2.0</TYPE>
<CONTENT>
<OWNER>
<ID>939KDKD393KD</ID>
<NAME>Universal</NAME>
<PUBLICKEY></PUBLICKEY>
<OWNER>
<LICENSEE>
<NAME>Arnold</NAME>
<ID>939KDKD393KD</ID>
<PUBLICKEY></PUBLICKEY>
</LICENSEE>
<PRINCIPAL TYPE==AND=>
<PRINCIPAL TYPE==OR=>
<PRINCIPAL>
<TYPE>x86Computer</TYPE>
<ID>3939292939d9e939</ID>
<NAME>Personal Computer</NAME>
<AUTHTYPE>Intel Authenticated Boot PC SHA-1
DSA512</AUTHTYPE>
<AUTHDATA>29293939</AUTH DATA>
<PRINCIPAL>
<PRINCIPAL>
<TYPE>Application</TYPE>
<ID>2939495939292</ID>
<NAME>Windows Media Player</NAME>
<AUTHTYPE>Authenticode SHA-1 </AUTHTYPE>
<AUTHDATA>93939</AUTHDATA>
<PRINCIPAL>
<PRINCIPAL>
<PRINCIPAL>
<TYPE>Person</TYPE>
<ID>39299482010</ID>
<NAME>Arnold Blinn</NAME>
<AUTHTYPE>Authenticate user</AUTHTYPE>
<AUTHDATA>\redmond\arnoldb</AUTHDATA>
<PRINCIPAL>
<PRINCIPAL>
<DRLTYPE>Simple</DRLTYPE>[the language tag 54]
<DRLDATA>
<START>19980102 23:20:14Z</START>
<END>19980102 23:20:14Z</END>
<COUNT>3</COUNT>
<ACTION>PLAY</ACTION>
<DRLDATA>
<ENABLINGBITS>aaaabbbbccccddd</ENABLINGBITS>
<DATA>
<SIGNATURE>
<SIGNERNAME>Universal</SIGNERNAME>
<SIGNERID>9382ABK3939DKD</SIGNERID>
<HASHALGORITHMID>MD5 </HASHALGORITHMID>
<SIGNALGORITHMID>RSA 128</SIGNALGORITHMID>
<SIGNATURE>xxxxyyxxxxyyxxxxyy</SIGNATURE>
<SIGNERPUBLICKEY></SIGNERPUBLICKEY>
<CONTENTSIGNEDSIGNERPUBLICKEY></CONTENTSIGNEDSIGNERPUBLICKEY>
<SIGNATURE>
<LICENSE>
<LICENSE>
<DATA>
<NAME>Beastie Boy's Play</NAME>
<ID>39384</ID>
<DESCRIPTION>Play the song unlimited</DESCRIPTION>
<TERMS></TERMS>
<VALIDITY>
<NOTBEFORE>19980102 23:20:14Z</NOTBEFORE>
<NOTAFTER>19980102 23:20:14Z</NOTAFTER>
<VALIDITY>
<ISSUEDDATE>19980102 23:20:14Z</ISSUEDDATE>
<LICENSORSITE>http://www.foo.Com</LICENSORSITE>
<CONTENT>
<NAME>Beastie Boy's</NAME>
<ID>392</ID>
```

-continued

```

<KEYID>39292</KEYID>
<TYPE>MS Encrypted ASF 2.0</TTYPE>
</CONTENT>
<OWNER>
<ID>939KDKD393KD</ID>
<NAME>Universal</NAME>
<PUBLICKEY></PUBLICKEY>
</OWNER>
<LICENSEE>
<NAME>Arnold</NAME>
<ID>939KDKD393KD</ID>
<PUBLICKEY></PUBLICKEY>
</LICENSEE>
<DRLTYPE>Script</DRLTYPE> [the language tag 54]
<DRLDATA>
function on_enable(action, args) as boolean
result = False
if action = "PLAY" then
result = True
end if
on_action = False
end function
...
</DRLDATA>
<DATA>
<SIGNATURE>
<SIGNERNAME>Universal</SIGNERNAME>
<SIGNERID>9382</SIGNERID>
<SIGNERPUBLICKEY></SIGNERPUBLICKEY>
<HASHID>MDS</HASHID>
<SIGNID>RSA 128</SIGNID>
<SIGNATURE>xxxxxxxxxxxxxx</SIGNATURE>
<CONTENTSIGNEDSIGNERPUBLICKEY></CONTENTSIGNEDSIGNERPUBLICKEY>
<SIGNATURE>
</LICENSE>

```

[0236] In the two DRLs 48 specified above, the attributes listed have the following descriptions and data types:

-continued

Attribute	Description	Data Type	Attribute	Description	Data Type
Id	ID of the license	GUID	Enabling Bits	These are the bits that enable access to the actual content. The interpretation of these bits is up to the application, but typically this will be the private key for decryption of the content. This data will be base-64 encoded. Note that these bits are encrypted using the public key of the individual machine.	String
Name	Name of the license	String	Signer Id	ID of person signing license	GUID
Content Id	ID of the content	GUID	Signer Name	Name of person signing license	String
Content Key Id	ID for the encryption key of the content	GUID	Signer Public Key	Public key for person signing license. This is the base-64 encoded public key for the signer.	String
Content Name	Name of the content	String	Content Signed Signer Public Key	Public key for person signing the license that has been signed by the content server private key. The public key to verify this signature will be encrypted in the content. This is base-64 encoded.	String
Content Type	Type of the content	String	Hash Alg Id	Algorithm used to generate hash. This is a string, such as "MDS".	String
Owner Id	ID of the owner of the content	GUID	Signature Alg Id	Algorithm used to generate signature. This is a string, such as "RSA 128".	String
Owner Name	Name of the owner of the content	String	Signature	Signature of the data. This is base-64 encoded data.	String
Owner Public Key	Public key for owner of content. This is a base-64 encoded public key for the owner of the content.	String			
Licensee Id	Id of the person getting license. It may be null.	GUID			
Licensee Name	Name of the person getting license. It may be null.	String			
Licensee Public Key	Public key of the licensee. This is the base-64 encoded public key of the licensee. It may be null.	String			
Description	Simple human readable description of the license	String			
Terms	Legal terms of the license. This may be a pointer to a web page containing legal prose.	String			
Validity Not After	Validity period of license expiration	Date			
Validity Not Before	Validity period of license start	Date			
Issued Date	Date the license was issued	Date			
DRL Type	Type of the DRL. Example include "SIMPLE" or "SCRIPT"	String			
DRL Data	Data specific to the DRL	String			

[0237] Methods

[0238] As was discussed above, it is preferable that any language engine 52 and any DRL language support at least

a number of specific license questions that the digital license evaluator 36 expects to be answered by any DRL 48. Recognizing such supported questions may include any questions without departing from the spirit and scope of the present invention, and consistent with the terminology employed in the two DRL 48 examples above, in one embodiment of the present invention, such supported questions or ‘methods’ include ‘access methods’, ‘DRL methods’, and ‘enabling use methods’, as follows:

[0239] Access Methods

[0240] Access methods are used to query a DRL 48 for top-level attributes.

[0241] VARIANT QueryAttribute (BSTR key)

[0242] Valid keys include License.Name, License.Id, Content.Name, Content.Id, Content.Type, Owner.Name, Owner.Id, Owner.PublicKey, Licensee.Name, Licensee.Id, Licensee.PublicKey, Description, and Terms, each returning a BSTR variant; and Issued, Validity.Start and Validity.End, each returning a Date Variant.

[0243] DRL Methods

[0244] The implementation of the following DRL methods varies from DRL 48 to DRL 48. Many of the DRL methods contain a variant parameter labeled ‘data’ which is intended for communicating more advanced information with a DRL 48. It is present largely for future expandability.

[0245] Boolean IsActivated(Variant data)

[0246] This method returns a Boolean indicating whether the DRL 48/license 16 is activated. An example of an activated license 16 is a limited operation license 16 that upon first play is active for only 48 hours.

[0247] Activate(Variant data)

[0248] This method is used to activate a license 16. Once a license 16 is activated, it cannot be deactivated.

[0249] Variant QueryDRL(Variant data)

[0250] This method is used to communicate with a more advanced DRL 48. It is largely about future expandability of the DRL 48 feature set.

[0251] Variant GetExpires(BSTR action, Variant data)

[0252] This method returns the expiration date of a license 16 with regard to the passed-in action. If the return value is NULL, the license 16 is assumed to never expire or does not yet have an expiration date because it hasn’t been activated, or the like.

[0253] Variant GetCount(BSTR action, Variant data)

[0254] This method returns the number of operations of the passed-in action that are left. If NULL is returned, the operation can be performed an unlimited number of times.

[0255] Boolean IsEnabled(BSTR action, Variant data)

[0256] This method indicates whether the license 16 supports the requested action at the present time.

[0257] Boolean IsSunk(BSTR action, Variant data)

[0258] This method indicates whether the license 16 has been paid for. A license 16 that is paid for up front would

return TRUE, while a license 16 that is not paid for up front, such as a license 16 that collects payments as it is used, would return FALSE.

[0259] Enabling Use Methods

[0260] These methods are employed to enable a license 16 for use in decrypting content.

[0261] Boolean Validate (BSTR key)

[0262] This method is used to validate a license 16. The passed-in key is the black box 30 public key (PU-BB) encrypted by the decryption key (KD) for the corresponding digital content 12 (i.e., (KD(PU-BB))) for use in validation of the signature of the license 16. A return value of TRUE indicates that the license 16 is valid. A return value of FALSE indicates invalid.

[0263] int OpenLicense 16(BSTR action, BSTR key, Variant data)

[0264] This method is used to get ready to access the decrypted enabling bits. The passed-in key is (KD(PU-BB)) as described above. A return value of 0 indicates success. Other return values can be defined.

[0265] BSTR GetDecryptedEnablingBits (BSTR action, Variant data) Variant GetDecryptedEnablingBitsAsBinary (BSTR action, Variant Data)

[0266] These methods are used to access the enabling bits in decrypted form. If this is not successful for any of a number of reasons, a null string or null variant is returned.

[0267] void CloseLicense (BSTR action, Variant data)

[0268] This method is used to unlock access to the enabling bits for performing the passed-in action. If this is not successful for any of a number of reasons, a null string is returned.

[0269] Heuristics

[0270] As was discussed above, if multiple licenses 16 are present for the same piece of digital content 12, one of the licenses 16 must be chosen for further use. Using the above methods, the following heuristics could be implemented to make such choice. In particular, to perform an action (say ‘PLAY’) on a piece of digital content 12, the following steps could be performed:

[0271] 1. Get all licenses 16 that apply to the particular piece of digital content 12.

[0272] 2. Eliminate each license 16 that does not enable the action by calling the IsEnabled function on such license 16.

[0273] 3. Eliminate each license 16 that is not active by calling IsActivated on such license 16.

[0274] 4. Eliminate each license 16 that is not paid for up front by calling IsSunk on such license 16.

[0275] 5. If any license 16 is left, use it. Use an unlimited-number-of-plays license 16 before using a limited-number-of-plays license 16, especially if the unlimited-number-of-plays license 16 has an expiration date. At any time, the user should be allowed to select a specific license 16 that has already been acquired, even if the choice is not cost-effective. Accordingly, the

user can select a license 16 based on criteria that are perhaps not apparent to the DRM system 32.

[0276] 6. If there are no licenses 16 left, return status so indicating. The user would then be given the option of:

[0277] using a license 16 that is not paid for up front, if available;

[0278] activating a license 16, if available; and/or

[0279] performing license acquisition from a license server 24.

[0280] Secure DRM Processor Architecture

[0281] Referring now to FIG. 13, it is to be appreciated that in one mode of obtaining and rendering digital content 12, such digital content 12 is downloaded or otherwise placed on a personal computer 60 or the like, and the corresponding digital license 16 once obtained is also downloaded or otherwise placed on the personal computer 60 or the like. Thereafter, the content 12 and the license 16 (or a sub-license based thereon) are downloaded from the computer 60 to a portable computing device 62. For example, the portable device 62 may be a portable audio or multimedia player such as the DIAMOND RIO portable player, marketed by S3 Incorporated of Santa Clara, Calif. Notably, such two-step transfer of the content 12 is not essential to the present invention. Accordingly, for the purpose of the present invention, the content 12 may come from an arbitrary source.

[0282] Designing and configuring a portable device 62 to support the DRM architecture as set forth above raises several issues. At least some of such issues are dealt with in U.S. patent application No. 09/_____, entitled "Binding a Digital License to a Portable Device or the Like in a Digital Rights Management (DRM) System and Checking Out/Checking In the Digital License to/from the Portable Device or the Like" and filed concurrently herewith under Attorney Docket No. MSFT-310/164266.1, hereby incorporated by reference herein in its entirety.

[0283] As was pointed out in such application, all obtaining of digital content 12 and a corresponding digital license or sub-license (hereinafter 'license') 16 for the portable device 62 is performed by way of a computer 60 or the like. Thus, the portable device 62 and the DRM system 32p (FIG. 13) therein need not include such functionality therein, except insofar as is necessary to download the content 12 and the license 16. Accordingly, significant license acquisition and content acquisition portions of the DRM system 32 as resident on the computer 60 may be omitted from the DRM system 32p as resident on the portable device 62.

[0284] As was also pointed out, the portable device 62 may be defined as a generally closed device in that data can be on-loaded and off-loaded only in a limited manner, user access to hardware within the portable device 62 is very limited, and input and display functionality is limited to a few function keys and perhaps a small LCD screen, respectively. Thus, a content thief can do very little in the way of examining either the memory or physical contents of the portable device 62 to obtain content 12 therein in an unencrypted form or decryption keys. In contrast, the computer 60 may be defined as a generally open device in that data can be on-loaded and off-loaded in a wide-ranging manner by any of a broad range of hardware and/or software, user

access to hardware within the portable device 62 is not limited in any significant way, and input and display functionality is available by way of a full-function keyboard, a mouse, a high-resolution monitor, and the like. Thus, a content thief has many potential opportunities available to examine the memory and physical contents of the computer 60 to obtain content 12 therein in an unencrypted form or decryption keys. In sum, then, the portable device 62 as a closed device is less susceptible to nefarious actions committed by a content thief, especially as compared to the computer 60 as an open device.

[0285] As a result, and also importantly, the portable device 62 and the DRM system 32p therein need not include functionality necessary to guard against most types of content theft and decryption key theft, except insofar as is necessary during download of the content 12 and the sub-license 16. Accordingly, significant theft prevention portions of the DRM system 32 as resident on the computer 60 may be omitted from the DRM system 32p as resident on the portable device 62 for the reason that functions such as hiding secrets, protecting integrity, isolating memory, and the like, while still necessary, are provided by the hardware mechanisms, which make the portable device a closed device. In contrast, on an open device such functions are typically implemented/approximated/simulated by means of software tamper-resistance.

[0286] To sum up, then, the DRM system 32p as resident on the portable device 62 need only include functionality necessary (1) to authenticate the portable device 62 to the computer 60 during downloading of a sub-license 16s to the portable device and at other appropriate times, and to facilitate such downloading, and (2) to render content 12 on the portable device 62 according to downloaded and resident license(s) 16, including ensuring that requirements in a license 16 are filled and obtaining the content key (KD) from the license 16. All other functionality as available in the DRM system 32 on the computer 60 is either unnecessary in the DRM system 32p on the portable device 62, or is inherent in the portable device 62 being a closed device.

[0287] However, and importantly, such other functionality is either unnecessary or inherent as discussed above only if the portable device 62 and specifically the processor 64 thereon can be trusted. That is to say, the portable device 62 and the processor 64 thereon must be of a type that substantially completely prevents a content thief from performing nefarious acts that would allow obtaining of content 12 therein in an unencrypted form or decryption keys. Accordingly, in one embodiment of the present invention, the processor 64 is a secure processor having an architecture as disclosed below. In particular, in one embodiment of the present invention, the secure processor 64 is constructed to run only authorized code. Note that the secure processor 64 and the architecture thereof of the present invention, though particularly applicable to a portable device 62, are not limited to such portable device 62. Instead, such secure processor 64 and architecture thereof may be employed in any type of computing device 14 without departing from the spirit and scope of the present invention.

[0288] In addition to running authorize code only, the secure processor 64 of the present invention ensures data privacy in that data on the portable device 62 associated with a particular application on the device 62 can be kept secret

from any other application on the device 62. Such data may be any data, and for example may include passwords, account numbers, private cryptographic keys, financial or other private data, and other sensitive personal information. Generally, in the present invention, the security processor 64 is operated to maintain a strict cryptographic separation between applications operating systems.

[0289] In the present invention, generally, the security of the processor 64 is based on the use of a security kernel 68 in the processor 64. Such security kernel 68 provides relevant higher-level functionality including protection from hostile code (e.g. a virus), authentication to a remote host (e.g. a DRM license server 24), certification of upgrades, and piracy protection for software on the portable device 62.

[0290] In the present invention, the secure processor 64 is constructed to include a security (CPU) key 66 physically hard-wired (permanently stored) thereto, and the security kernel 68 is also physically hard-wired thereto, where only the security kernel 68 can access the CPU key 66. Such physical hard-wiring may be performed during manufacturing of the secure processor 64 and may be done in any appropriate manner without departing from the spirit and scope of the present invention. Such physical hardwiring is known or should be apparent to the relevant public and therefore need not be described herein in any detail. For example, the secure processor 64 may be manufactured with storage space 70 for a CPU key 66 and a security kernel 68, where the storage space 70 is in the form of ROM to be pre-programmed by the manufacturer. Such ROM may comprise, at least in part, fused memory locations. Thus, as a final manufacturing step, selected ones of the fused memory locations in the storage space 70 are ‘blown’ to permanently instantiate a particular CPU key 66 and a particular security kernel 68.

[0291] In the present invention, the secure processor 64 is operable in a normal mode and a preferred mode, where the security kernel 68 can access the CPU key 66 only during the preferred mode. For example, the processor 64 may be manufactured with a physical switch (such as an electronic gate) that allows the CPU key 66 to be read only when the processor 64 is in preferred mode. As may be appreciated, the security kernel 68 employs the accessed CPU key 66 during the preferred mode to instantiate and/or authenticate a secure application 72 such as a DRM system 32p, a banking/financial system, etc. on the portable device 62. The security kernel 68 may automatically instantiate a particular secure application, may authenticate a secure application instantiated by another process, or may initially instantiate a secure chooser application 72c that allows a user to select from one or more available secure applications 72 on the portable device 62.

[0292] In any case, the accessed CPU key 66 is employed by the security kernel 68 to decrypt one or more encrypted security keys for the application 72 instantiated. For example, in the case where the security kernel 68 instantiates/authenticates the DRM system 32p on the portable device 62, it may be that at least the black box private key PR-BB for the DRM system 32p is already encrypted according to the CPU key 68 and stored on the portable device 62 as CPU(PR-BB), and the security kernel during the preferred mode employs the accessed CPU key 66 to decrypt CPU(PR-BB) to produce (PR-BB) such that (PR-

BB) is available to the instantiated DRM system 32p. Such CPU key 66 may also encrypt one or more n intermediate keys which in turn encrypt (PR-BB), as seen below. As may be appreciated, then, the CPU key 66 is the key to unlocking or decrypt the secrets identified with each application 72, and therefore must be well-protected.

[0293] In the present invention, then, the security kernel 68 ensures that each application 72 has access to the secrets of such application 72, and does not have access to the secrets of any other application 72. As a result, each application 72 on the portable device 62 is isolated from every other application 72 on the portable device 62. Such functionality is required for banking applications (credit card numbers, PINs, e.g.) and DRM applications (private keys, e.g.).

[0294] In addition, the accessed CPU key 66 and/or the decrypted key(s) may be employed by the security kernel 68 to authenticate/verify the application 72 to be instantiated. In particular, the application 72 may include a certificate or the like, and the security kernel 72 may perform a hash or MAC (message authentication code) over the code for the application based on the CPU key 66 and then compare the hash or MAC to the certificate or the like. Details of the hash depend on whether public-key (asymmetric) or symmetric cryptography is employed, as discussed in more detail below. As may be appreciated, any appropriate hash function may be employed without departing from the spirit and scope of the present invention. Hash functions are generally known or should be appreciated by the relevant public and therefore need not be described herein in any detail.

[0295] If the compare fails, the security kernel 72 may refuse to instantiate/authenticate the application 72 or may instantiate or allow instantiation but not decrypt the secrets for the application 72, for example. As may be appreciated, by having the security kernel 68 authenticate/verify an application 72 based on a performed hash, the security kernel 68 ensures that system resources on the portable device 62 (in particular, the application-specific secrets) are restricted to an authorized application 72.

[0296] In one embodiment of the present invention, and referring now to FIG. 14, the security processor 64 enters preferred mode whenever a predefined initializing processor action is performed. For example, the security processor 64 may enter preferred mode whenever a CPU reset is performed, thus making the CPU key 66 accessible by the security kernel 68 (step 1401). As may be appreciated, a CPU reset is a typical processor operation that places a processor in an initialized state without necessarily erasing all memory on the processor 62. As may be appreciated, such attribute is desirable in instances where certain data from prior to a CPU reset is necessary after such CPU reset.

[0297] The CPU reset may preferably be performed either manually such as at initial power-up of the processor 64, or programmatically such as by program code running on the processor 64. In one embodiment of the present invention, upon the CPU reset, data in cache 74 on the processor 64 is erased (step 1403). Thus, any data previously stored in the cache 74 is not available during preferred mode to interfere with preferred mode processes, and in particular any data previously stored in the cache 74 cannot be employed to get at the CPU key 66 or subvert the execution of the security kernel 68. With such erasure, then, a content or data thief

intending to perform a nefarious act such as identifying the CPU key 66 during preferred mode cannot place a malicious program in cache 74, enter preferred mode, and expect to run the malicious program during preferred mode. Quite simply, the malicious program is erased as part of erasing the cache 74.

[0298] Once the cache is erased, the security kernel 68 is then run (step 1405). As may be appreciated, the security kernel 68 is run by loading same from the storage space 70 onto the processor 64 and then performing the program code incumbent in such security kernel 68. Typically, the storage space 70 with regard to the security kernel 68 is processor ROM and not some secondary storage medium such as a hard disk, or flash memory, although the present invention is not restricted in this regard.

[0299] Generally, the program code of the security kernel 68 as performed accesses the CPU key 66 at a predetermined memory location in the storage space 70 (step 1407), and then applies the accessed CPU key 66 to decrypt the one or more encrypted security keys for the application to be instantiated (step 1409), as was discussed above. Presumably, such key(s) have already been encrypted according to the CPU key 68 and stored in the storage space 70. Thereafter, the program code of the security kernel 68 stores the decrypted key(s) on the portable device 62 in a location where the application to be instantiated expects the key(s) to be found (step 1410).

[0300] In addition, the program code of the security kernel 68 instantiates, causes instantiation or allows the instantiation of the application on the portable device 62 (step 1413). Performing such instantiation, is generally known or should be apparent to the relevant public and therefore need not be described herein in any detail. Accordingly, any particular form of instantiation maybe performed without departing from the spirit and scope of the present invention. Such instantiation or loading comprises placing executable code and data into a memory space, such that the code can be executed. In principle, this can be a complex task and may involve things, such a resolving dependencies (by loading other DLLs) or relocation (changing certain addresses in the code). Notably, loading in itself is not critical to security and does not necessarily have to be performed by the security kernel 68. The critical task for the security kernel 68 is instead authentication of the loaded image. That is, the security kernel 68 has to ensure that the result of the loading (or instantiation) is what it claims to be.

[0301] As mentioned above, the application 72 to be instantiated may be authenticated/verified according to the CPU key 68 and/or the decrypted key(s) (step 1411). In such case, prior to or after instantiation, the program code of the security kernel 68 employs the accessed CPU key 66 and/or the decrypted key(s) to perform a hash or MAC over the code for the application 72 to be instantiated and then compares the hash or MAC to a certificate or the like accompanying the application 72. If the compare fails, the security kernel 72 may refuse to instantiate the application 72 or may instantiate but not decrypt the secrets for the application 72 as at step 1409. If the secrets are already decrypted, the security kernel 72 may decide to delete the decrypted secrets.

[0302] Once the security kernel finishes instantiating/authenticating the application, the processor 64 enters normal

mode and the CPU key 66 becomes inaccessible (step 1415). Entering normal mode may occur automatically upon the security kernel 68 finishing or may occur by an instruction in the security kernel 68.

[0303] In one embodiment of the present invention, upon entering normal mode, data in the cache 74 on the processor 64 is once again erased (step 1417). Thus, any sensitive data in the cache 74 from preferred mode operations, such as for example the CPU key 66 or a secret for an application 72 as derived from the CPU key 66, is not available during normal mode to be read by a content or data thief. Note that erasing cache 74 both at steps 1403 and 1417 may also encompass zeroing registers and writing zero or random values to memory locations that contain information derived from the CPU key. Note that both the memory locations themselves and any transient copies must be erased.

[0304] Referring now to FIG. 15, it is seen that in the case where the security kernel 68 initially instantiates/authenticates a secure chooser application 72c that allows a user to select from one or more available secure applications 72 on the portable device 62, the security kernel 68 employs such chooser application 72c and a stored chooser value 76 that is persistent and that is accessible to the security kernel 68 to select from among at least one other application 72 available on the portable device 62. Importantly, each time the processor 64 enters the preferred mode and runs the security kernel 68, such security kernel 68 checks the chooser value 76 and instantiates/authenticates a particular application 72, 72c corresponding to the chooser value. For example, if the chooser value 76 is set to 0, the security kernel 68 instantiates/authenticates the chooser application 72c. Similarly, if the chooser value 76 is set to 1, 2, or 3, the security kernel 68 instantiates/authenticates a first, second, or third application 72, respectively.

[0305] In employing the chooser application 72c and the chooser value 76, it is seen that upon initial power-up of the processor 64, the chooser value 76 is set to the value corresponding to the chooser application 72c (0 in the above example) (step 1501). Thus, upon a power-up CPU reset, the processor 64 enters the preferred mode and runs the security kernel 68, the security kernel checks the chooser value 76 and finds it to be 0, and the security kernel 68 instantiates/authenticates the corresponding chooser application 72c (steps 1503, 1505). Thereafter, the processor 64 enters the normal mode and the instantiated chooser application 72c is left to run on the portable device 62 (step 1507). As may be appreciated, the chooser application 72c presents a number of applications 72 for selection by a user of the portable device 62, and the user thus selects one of the presented applications 72 to be instantiated on the portable device 62 (step 1509). Note that the presentation of the applications 72 to the user may be done in any appropriate manner without departing from the spirit and scope of the present invention. For example, the portable device 62 may present the applications 72 on a display (not shown) on the portable device 62, or the applications may be hard-wired into labeled selection buttons (not shown) on the portable device 62.

[0306] Upon user selection of an application 72 to be instantiated, the chooser application 72c sets the chooser value 76 to the value corresponding to the selected application 72 (1, e.g.) (step 1511), and executes a CPU reset (step 1513). Importantly, the chooser value 76 is persistent

in that the chooser value 76 is not erased by the CPU reset. That is, the chooser value 76 is preferably stored in a memory location not affected by a CPU reset so as to be available after the CPU reset.

[0307] As may now be appreciated, after the CPU reset is executed by the chooser application 72c, the processor 64 enters the preferred mode and runs the security kernel 68, the security kernel checks the chooser value 76 and finds it to be 1, and the security kernel 68 instantiates/authenticates the corresponding chosen application 72 (steps 1515, 1517). Thereafter, the processor 64 enters the normal mode and the instantiated chosen application 72c is left to run on the portable device 62 (step 1519).

[0308] In one embodiment of the present invention, upon the selected application 72 being instantiated and run by the security kernel 68, either the security kernel 68 (prior to the processor entering normal mode) or the chosen application 72 (after the processor enters normal mode) sets the chooser value 76 back to the value corresponding to the chooser application 72 (0 in the present example) (step 1521). Thus, upon execution of another CPU reset (step 1523) from whatever source, the security kernel 68 once again instantiates/authenticates the chooser application 72c to begin the selection process anew. Once again, the chooser value 76, being persistent, is not erased by the CPU reset and is available after the CPU reset.

[0309] Notably, the chooser value 76 does not have to be an integer. In principle, the chooser value 76 could be the entire instantiated (loaded) image or program. In this case, the last running program loads the next program and then sets off the special CPU instruction, which triggers preferred mode.

[0310] Secure DRM Processor—Symmetric Cryptography and the Code Image

[0311] In one embodiment of the present invention, and as alluded to above, the security kernel 68 does not have public key/private key encryption and decryption capabilities. Instead, the security kernel 68 implements a MAC (message authentication code) and a symmetric cipher, and the CPU key 66 is therefore a symmetric key. In such embodiment, and referring now to FIG. 16, each application 72 on the portable device 62 exists in the form of a corresponding code image 78 that is constituted at least in part to facilitate symmetric encryption and decryption.

[0312] To constitute the code image 78, and in one embodiment of the present invention, there is a manufacturer-specific device key KMAN which is unique to each portable device 62 but independent of the CPU key 66. The purpose of KMAN is to allow each device manufacturer to administrate its device secrets independently. In particular, and as will be seen, KMAN frees the manufacturer of the processor 64 from the burden of maintaining a secret database associated with each manufactured processor 64.

[0313] With KMAN, each code image 78 for the portable device 62 has a header 80 and a main body 82. In particular, the header 80 has the following form, where KCPU is the CPU key 66 and KCODE is the key secret of the corresponding application 72:

KCPU (KMAN)	KMAN encrypted according to KCPU
MAC (main body 82, KMAN)	message authentication code of the main body 82 under KMAN
KMAN (KCODE)	KCODE encrypted according to KMAN

[0314] Note that the MAC may also be based on KMAN-KCODE.

[0315] When called to load a given code image 78, and referring now to FIG. 17, the security kernel 68 performs the following steps related to the header 80 of the code image 78:

[0316] 1. Apply KCPU to KCPU (KMAN) to produce KMAN (step 1701);

[0317] 2. Compute MAC (main body 82, KMAN) (step 1703);

[0318] 3. Compare computed MAC (main body 82, KMAN) to MAC (main body 82, KMAN) from the header 80 to determine if the code image 78 has been corrupted, modified, adulterated, etc. (step 1705); and

[0319] 4. Assuming the MACs match, Apply KMAN to KMAN (KCODE) to produce KCODE (step 1707).

[0320] As may be appreciated, the manufacturer of the portable device 62 must have access to the CPU key 66 (KCPU) to generate the header 80 of the code image 78. However, such CPU key 66 is never revealed outside the processor 64. In one embodiment of the present invention, this apparent contradiction is resolved by providing the processor 64 with a third, production mode during which the CPU key 66 is externally accessible to the manufacturer of the portable device 62.

[0321] In such embodiment, and referring now to FIG. 18, the processor 64 is manufactured and shipped to the manufacturer of the portable device 62 in production mode (step 1801), and the manufacturer of the portable device 62 accesses the CPU key 66 of the processor 64 in production mode (step 1803). Such manufacturer then generates the header 80 for each code image 78 for the processor 64 portable device 62 based on the accessed CPU key 66 (KCPU), KMAN, and the main body 82 (step 1805).

[0322] Importantly, at some point prior to shipping the portable device 62 to a consumer or to be purchased by a consumer, the manufacturer of the portable device 62 permanently disables production mode for the processor 64 within the portable device (step 1807). Thus, such consumer cannot actuate such production mode to access the CPU key 66. Note that permanent disablement of production mode for the processor 64 may be performed prior to or after loading code images 78 (step 1809) onto the portable device 62 that are generated based on the accessed CPU key 66.

[0323] Permanently disabling such production mode may be done in any appropriate manner without departing from the spirit and scope of the present invention. For example, the processor 64 may be constructed with a fuse 84 (FIG. 13) or the like, and the fuse 13 may be ‘blown’ to permanently disable production mode. Such permanent disabling is known or should be apparent to the relevant public and therefore need not be described herein in any detail.

[0324] Secure DRM Processor—Asymmetric Cryptography and the Code Image

[0325] In one embodiment of the present invention, and as also alluded to above, the security kernel 68 does have public key/private key encryption and decryption capabilities. Here, the security kernel 68 implements a hash and public-key operations (encryption, decryption, signing, signature verification), and the CPU key 66 is therefore the private key of a public key—private key pair. In such embodiment, and referring now to FIG. 19, each application 72 on the portable device 62 exists in the form of a corresponding code image 78 that is constituted at least in part to facilitate asymmetric encryption and decryption.

[0326] To constitute the code image 78 in this instance, and in one embodiment of the present invention, only the CPU key 66 (private key) need be employed rather than such CPU key 66 and the aforementioned manufacturer-specific device key KMAN. As may be appreciated, this is because the CPU key 66 is a private key and a separate corresponding public key is employed by the external world. Put another way, and as should be appreciated, the asymmetric nature of the internal or private CPU key 66 and the corresponding external or public key imparts such keys with the functionality necessary to perform all encryption without any other keys.

[0327] In one embodiment of the present embodiment, each code image 78 for the portable device 62 still has a header 80 and a main body 82. However, with the public key—private key pair including the CPU key 66 as the private key thereof, and without the need for KMAN as above, the header 80 has the following simplified form, where KCPU is the CPU key 66 and KCODE is the key secret of the corresponding application 72:

public key (HASH (main body 82), Hash of both the main body 82 and KCODE)	KCODE, both encrypted according to the public key
---	---

[0328] Importantly, in both the symmetric case above and the asymmetric case here, only the security kernel 68 can get to KCODE, inasmuch as only the security kernel 68 can access the private key (CPU key 66) corresponding to the public key, as was discussed above. Also importantly, since only the security kernel 68 can access the private key (CPU key 66) corresponding to the public key, KCODE is tied to the security kernel 68, the CPU key 66, and the portable device 62. As tied, and as should be appreciated, KCODE cannot be transferred over to another portable device 62/security kernel 68 and be employed thereon.

[0329] Also importantly, KCODE is tied to the executable image 78 to which it belongs. Assuming that different images 78/programs on the device 62 do not trust each other, KCODE for one image 78 should not be accessible by any entity other than the application instantiated from such image. Thus, the image 78 of an application to be instantiated should only be able to access its KCODE if it is unadulterated and unmodified, as shown by a hash comparison. If only a single bit in the image 78 has been changed, the image 78 is not to be trusted and should not be able to access its KCODE.

[0330] Thus, when called to load a given code image 78, and referring now to FIG. 20, the security kernel 68 performs the following steps related to the header 80 of the code image 78:

[0331] 1. Compute HASH (main body 82) (step 2001);

[0332] 2. Apply private key to public key (HASH (main body 82), KCODE) to produce HASH (main body 82) and KCODE (step 2003);

[0333] 3. Compare computed HASH to decrypted HASH to determine if the code image 78 has been corrupted, modified, adulterated, etc. (step 2005); and

[0334] 4. Assuming the HASHes match, employing the decrypted KCODE as appropriate (step 2007).

[0335] As may be appreciated, steps 2001-2007 more generally instantiate the functions of (1) verifying that the header 80 with KCODE therein belongs to the code image 78 and (2) exposing KCODE to the security kernel 68.

[0336] Of course, any other mechanism, symmetric or asymmetric, for tying KCODE to a security kernel 68 and to its code image 78 and limiting access to KCODE to the security kernel 68 and its code image 78 may be employed without departing from the spirit and scope of the present invention. As but one example, the header 80 may have the following simplified form:

public key (HASH (main body 82), Hash of both the main body 82 and KCODE)	KCODE, encrypted according to the public key
public key (KCODE)	KCODE, encrypted according to the public key

[0337] Of course, such header 80 requires two decryptions rather than one, as above.

[0338] As may be appreciated, use of an asymmetric public key—private key pair frees the manufacturer of the portable device 62 from having to access the CPU key 66 to generate the header 80 of the code image 78. Thus, such CPU key 66 truly never need be revealed outside the processor 64, and no production mode need be provided to the processor 64, as is the case above with regard to using a symmetric key as the CPU key 66.

[0339] With use of an asymmetric key pair, then, certified code images 78 may be produced without requiring special production modes or secret databases. The manufacturer of the portable device 62 simply uses the public-key corresponding to the CPU key 66 as a private key to produce the required header 80 for each code image 78. In fact, if the public key is indeed public, anybody can produce a code image 78 with a valid header 80.

[0340] Secure DRM Processor—Asymmetric and Symmetric Cryptography

[0341] Fast public key—private key cryptography code may require 10 to 20 kilobytes of memory space, which may be expensive for on-chip ROM or the like in a portable device 62. Thus, in one embodiment of the present invention, and referring now to FIG. 21, the security kernel 68 is a code security kernel 68c which uses symmetric cryptog-

raphy as described above, but only on a privileged code image 78 which implements an extended version of the security kernel 68e. The extended security kernel 68e in turn uses the public key—private key asymmetric cryptography as described above. Such extended security kernel 68e, then, is employed to load an arbitrary application 72 from a corresponding code image 78.

[0342] Conclusion

[0343] Notably, with a portable device 62 having a secure processor 64 and secure kernel 68 as disclosed above, protection of the security keys and other secrets is relegated from a black box—type device to the platform. Thus, the platform assures that an application gets a secret that is determined by the entirety of the running software stack. A license server 24 or sub-licensing process receiving a request from the platform sees a component with a certified key. The certification indicates that the key could only have come from a trusted device running a known software configuration. Hence the server 24 or process trusts the platform and issues the license 16 sub-license 16s. In a more generalized e-commerce case, a vendor receiving a request (to buy a product, to trade a stock, etc.) checks that the request is coming from a trusted device running a known software stack. The check succeeds because the certified key would only have been disclosed if the software stack was certified trusted, so the transaction is allowed.

[0344] The programming necessary to effectuate the processes performed in connection with the present invention is relatively straight-forward and should be apparent to the relevant programming public. Accordingly, such programming is not attached hereto. Any particular programming, then, may be employed to effectuate the present invention without departing from the spirit and scope thereof.

[0345] In the foregoing description, it can be seen that the present invention comprises a new and useful secure processor 64 and an architecture therefor that can be trusted to keep hidden a secret of the DRM system 32, especially in cases where the processor 64 is on a portable device 62 or the like. It should be appreciated that changes could be made to the embodiments described above without departing from the inventive concepts thereof. For example, although disclosed as being particularly relevant to a DRM system 32 on a portable device 62, the invention may also be employed on another system such as for example a banking system and/or may also be employed on a device other than a portable device 62 without departing from the spirit and scope of the present invention. It should be understood, therefore, that this invention is not limited to the particular embodiments disclosed, but it is intended to cover modifications within the spirit and scope of the present invention as defined by the appended claims.

1. A secure processor for a computing device, the processor being operable in a normal mode and a preferred mode, the processor including a security kernel for being instantiated on the processor when the processor enters into the preferred mode and a security key accessible by the instantiated security kernel when the processor is operating in the preferred mode, the security kernel employing the accessed security key during the preferred mode to authenticate a secure application on the computing device, wherein the security kernel allows the processor to be trusted to keep hidden a secret of the application.

2. The processor of claim 1 in combination with the application.

3. The processor of claim 2 wherein the application is selected from a group consisting of a digital rights management (DRM) system and a banking/financial system.

4. The processor of claim 1 wherein the security kernel automatically authenticates a particular application.

5. The processor of claim 1 wherein the security kernel initially authenticates a chooser application that allows a user to select from at least one available applications on the computing device.

6. The processor of claim 1 wherein the security kernel employs the accessed security key during the preferred mode to decrypt at least one encrypted key for the application.

7. The processor of claim 1 in combination with the computing device.

8. The processor of claim 7 wherein the computing device is a portable computing device.

9. The processor of claim 1 further comprising a storage space, the security kernel being permanently stored in the storage space.

10. The processor of claim 1 further comprising a storage space, the security key being permanently stored in the storage space.

11. The processor of claim 1 wherein the security kernel employs the accessed security key during the preferred mode to authenticate/verify the application prior to instantiation thereof.

12. The processor of claim 11 wherein the security kernel performs a hash/MAC (message authentication code) over at least a portion of the application and then compares the hash/MAC to a hash/MAC corresponding to the application.

13. The processor of claim 1 wherein such processor enters preferred mode whenever a predefined initializing processor action is performed.

14. The processor of claim 13 wherein such processor enters preferred mode whenever a CPU reset is performed.

15. A method for a secure processor to instantiate and authenticate a secure application thereon by way of a security kernel, the method comprising:

entering a preferred mode where a security key of the processor is accessible;

instantiating and running a security kernel, the security kernel:

accessing the security key;

applying the accessed security key to decrypt at least one encrypted key for the application;

storing the decrypted key(s) in a location where the application will expect the key(s) to be found; and

authenticating the application on the processor; and

entering a normal mode from the preferred mode after the security kernel authenticates the application, where the security key is not accessible;

wherein the security kernel allows the processor to be trusted to keep hidden the key(s) of the application.

16. The method of claim 15 wherein entering the preferred mode comprises entering the preferred mode upon a CPU reset.

17. The method of claim 15 further comprising erasing data in a cache of the processor prior to instantiating the security kernel.

18. The method of claim 15 further comprising erasing data in a cache of the processor after entering normal mode.

19. The method of claim 15 wherein the security kernel employs the accessed security key during the preferred mode to authenticate/verify the application prior to instantiation thereof.

20. The method of claim 19 wherein the security kernel performs a hash/MAC (message authentication code) over at least a portion of the application and then compares the hash/MAC to a hash/MAC corresponding to the application.

21. The method of claim 15 wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN; and

applying KMAN to KMAN (KCODE) to produce KCODE.

22. The method of claim 21 wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
MAC (main body, KMAN)	message authentication code of the main body under KMAN
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN;

computing MAC (main body, KMAN);

comparing the computed MAC to MAC (main body, KMAN) from the header to determine if the code image has been changed; and

if the MACs match, applying KMAN to KMAN (KCODE) to produce KCODE.

23. The method of claim 15 wherein the security key of the processor is a private key of a public key—private key pair and the application is instantiated from a code image including a main body and a header including:

public key (KCODE)	KCODE encrypted according to the public key
--------------------	---

where KCODE is the secret of the application, and
wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises applying the security key as the private key to public key (KCODE) to produce KCODE.

24. The method of claim 23 wherein the security key of the processor is a private key of a public key—private key pair and the application is instantiated from a code image including a main body and a header including:

public key (HASH (main body), KCODE)	Hash of the main body and KCODE, both encrypted according to the public key
--------------------------------------	---

where KCODE is the secret of the application, and
wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

computing HASH (main body);

applying the private key to public key (HASH (main body), KCODE) to produce HASH (main body) and KCODE;

comparing the computed HASH to the produced HASH to determine if the code image has been changed;; and

if the HASHes match, employing the produced KCODE as appropriate.

25. A method for a secure processor to instantiate one of a plurality of available secure applications thereon by way of a security kernel, the method comprising:

setting a chooser value to a value corresponding to a chooser application upon power-up;

entering a preferred mode upon a power-up CPU reset and instantiating the security kernel, the security kernel determining that the chooser value corresponds to the chooser application and therefore authenticating same, the chooser application being instantiated;

entering a normal mode after the chooser application is instantiated and leaving same to run, the chooser application presenting the plurality of available applications for selection by a user;

receiving a selection of one of the presented applications to be instantiated;

setting the chooser value to a value corresponding to the selected application;

entering a preferred mode upon an executed CPU reset and instantiating the security kernel, the security kernel determining that the chooser value corresponds to the selected application and therefore authenticating same, the selected application being instantiated;

entering a normal mode after the selected application is instantiated and leaving same to run;

wherein the security kernel allows the processor to be trusted to keep hidden a secret of the chooser application and a secret of the selected application.

26. The method of claim 25 further comprising setting the chooser value to the value corresponding to the chooser application upon the selected application being authenticated by the security kernel, wherein upon execution of a CPU reset, the security kernel determines that the chooser value corresponds to the chooser application 72c and therefore authenticates same.

27. The method of claim 25 further comprising storing the chooser value in a memory location not affected by a CPU reset so that the stored chooser value is available after same.

28. A method for a secure processor to instantiate a secure application thereon, the method comprising:

instantiating a first security kernel which employs symmetric cryptography;

instantiating by way of the instantiated first security kernel a second security kernel which employs asymmetric cryptography; and

authenticating by way of the instantiated second security kernel the secure application.

29. The method of claim 28 wherein the security key of the processor is a symmetric key and the second security kernel is instantiated by the first security kernel from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is a security key of the processor, KMAN is a device key independent of the security key, and KCODE is the private key of the second security kernel, and

wherein the first security kernel applies the security key to decrypt the private key of the second security kernel during instantiation thereof by:

applying KCPU to KCPU (KMAN) to produce KMAN; and

applying KMAN to KMAN (KCODE) to produce KCODE.

30. The method of claim 29 wherein the application is instantiated by the second security kernel from a code image including a main body and a header including:

public key (KCODE)	KCODE encrypted according to the public key
--------------------	---

where KCODE is the secret of the application, and

wherein the second security kernel applies the private key to decrypt the secret of the application during authentication thereof.

31. A computer-readable medium having stored thereon computer-executable instructions implementing a method for a secure processor to instantiate a secure application thereon by way of a security kernel, the method comprising:

entering a preferred mode where a security key of the processor is accessible;

instantiating and running a security kernel, the security kernel:

accessing the security key;

applying the accessed security key to decrypt at least one encrypted key for the application;

storing the decrypted key(s) in a location where the application will expect the key(s) to be found; and authenticating the application on the processor; and

entering a normal mode from the preferred mode after the security kernel authenticates the application, where the security key is not accessible;

wherein the security kernel allows the processor to be trusted to keep hidden the key(s) of the application.

32. The medium of claim 31 wherein entering the preferred mode comprises entering the preferred mode upon a CPU reset.

33. The medium of claim 31 wherein the method further comprises erasing data in a cache of the processor prior to instantiating the security kernel.

34. The medium of claim 31 wherein the method further comprises erasing data in a cache of the processor after entering normal mode.

35. The medium of claim 31 wherein the security kernel employs the accessed security key during the preferred mode to authenticate/verify the application prior to instantiation thereof.

36. The medium of claim 35 wherein the security kernel performs a hash/MAC (message authentication code) over at least a portion of the application and then compares the hash/MAC to a hash/MAC corresponding to the application.

37. The medium of claim 31 wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN; and

applying KMAN to KMAN (KCODE) to produce KCODE.

38. The medium of claim 37 wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
MAC (main body, KMAN)	message authentication code of the main body under KMAN
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN;

computing MAC (main body, KMAN);

comparing the computed MAC to MAC (main body, KMAN) from the header to determine if the code image has been changed; and

if the MACs match, applying KMAN to KMAN (KCODE) to produce KCODE.

39. The medium of claim 31 wherein the security key of the processor is a private key of a public key—private key pair and the application is instantiated from a code image including a main body and a header including:

public key (KCODE)	KCODE encrypted according to the public key
--------------------	---

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises applying the security key as the private key to public key (KCODE) to produce KCODE.

40. The medium of claim 39 wherein the security key of the processor is a private key of a public key—private key pair and the application is instantiated from a code image including a main body and a header including:

public key (HASH (main body), KCODE)	Hash of the main body and KCODE, both encrypted according to the public key
---	--

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

computing HASH (main body);

applying the private key to public key (HASH (main body), KCODE) to produce HASH (main body) and KCODE;

comparing the computed HASH to the produced HASH to determine if the code image has been changed;; and

if the HASHes match, employing the produced KCODE as appropriate.

41. A computer-readable medium having computer-executable instructions thereon implementing a method for a secure processor to instantiate one of a plurality of available secure applications thereon by way of a security kernel, the method comprising:

setting a chooser value to a value corresponding to a chooser application upon power-up;

entering a preferred mode upon a power-up CPU reset and instantiating the security kernel, the security kernel determining that the chooser value corresponds to the chooser application and therefore authenticating same, the chooser application being instantiated;

entering a normal mode after the chooser application is instantiated and leaving same to run, the chooser application presenting the plurality of available applications for selection by a user;

receiving a selection of one of the presented applications to be instantiated;

setting the chooser value to a value corresponding to the selected application;

entering a preferred mode upon an executed CPU reset and instantiating the security kernel, the security kernel determining that the chooser value corresponds to the selected application and therefore authenticating same, the selected application being instantiated;

entering a normal mode after the selected application is instantiated and leaving same to run;

wherein the security kernel allows the processor to be trusted to keep hidden a secret of the chooser application and a secret of the selected application.

42. The medium of claim 41 wherein the method further comprises setting the chooser value to the value corresponding to the chooser application upon the selected application being authenticated by the security kernel, wherein upon execution of a CPU reset, the security kernel determines that the chooser value corresponds to the chooser application 72c and therefore authenticates same.

43. The medium of claim 41 wherein the method further comprises storing the chooser value in a memory location not affected by a CPU reset so that the stored chooser value is available after same.

44. A computer-readable medium having stored thereon computer-executable instructions implementing a method for a secure processor to instantiate a secure application thereon, the method comprising:

instantiating a first security kernel which employs symmetric cryptography;

instantiating by way of the instantiated first security kernel a second security kernel which employs asymmetric cryptography; and

authenticating by way of the instantiated second security kernel the secure application.

45. The medium of claim 44 wherein the security key of the processor is a symmetric key and the second security kernel is instantiated by the first security kernel from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is a security key of the processor, KMAN is a device key independent of the security key, and KCODE is the private key of the second security kernel, and

wherein the first security kernel applies the security key to decrypt the private key of the second security kernel during instantiation thereof by:

applying KCPU to KCPU (KMAN) to produce KMAN; and

applying KMAN to KMAN (KCODE) to produce KCODE.

46. The medium of claim 45 wherein the application is instantiated by the second security kernel from a code image including a main body and a header including:

public key (KCODE)	KCODE encrypted according to the public key
--------------------	---

where KCODE is the secret of the application, and wherein the second security kernel applies the private key to decrypt the secret of the application during instantiation thereof.

* * * * *